Benutzerhandbuch

Acronis Privacy Expert 9.0 Corporate

Acronis

Compute with confidence

www.acronis.de

ACR06.APE9C-05-15.502

Copyright © Acronis, Inc., 2000-2006. Alle Rechte vorbehalten.

Acronis, Acronis Compute with Confidence, Acronis Snap Restore, Acronis Recovery Manager, Acronis Secure Zone und das Acronis-Logo sind eingetragene Warenzeichen von Acronis, Inc.

Linux ist ein eingetragenes Warenzeichen von Linus Torvalds.

Windows und MS-DOS sind eingetragene Warenzeichen der Microsoft Corporation.

Andere in diesem Buch erwähnte Namen können Warenzeichen oder eingetragene Warenzeichen der jeweiligen Eigentümer sein und sollten als solche betrachtet werden.

Die Veränderung und Verbreitung dieser Dokumentation ohne schriftliche Genehmigung des Copyright-Inhabers ist untersagt.

Die Verbreitung des Werkes oder einzelner Bestandteile des Werkes in beliebiger auf Papier abgedruckter Form (z.B. als Buch) zu kommerziellen Zwecken ist ohne vorherige schriftliche Genehmigung des Copyright-Inhabers verboten.

Diese Dokumentation wird ohne Anspruch auf Vollständigkeit zur Verfügung gestellt. Der Autor gewährleistet nicht, dass der Inhalt fehlerfrei ist, Ihren Anforderungen sowie dem von Ihnen gewünschten Einsatzzweck entspricht. Weiterhin übernimmt der Autor keine Gewähr für die Richtigkeit des Inhaltes, soweit nicht grob fahrlässiges oder vorsätzliches Verhalten vorliegt. Teile oder die gesamte Dokumentation können jederzeit ohne Ankündigung geändert werden.

Inhaltsverzeichnis

KAPITEL 1. INSTALLATION 10
1.1 SYSTEMANFORDERUNGEN UND UNTERSTÜTZTE BETRIEBSSYSTEME 10
1.2 SICHERHEITSPARAMETER FÜR ACRONIS PRIVACY EXPERT CORPORATE EINSTELLEN 10
1.3 ALLGEMEINE FUNKTIONSWEISE 11
1.4 ACRONIS LICENSE SERVER 12
1.5 LOKALE INSTALLATION DER KOMPONENTEN 17
1.6 ACRONIS-KOMPONENTEN AUF REMOTE-COMPUTERN INSTALLIEREN 18
1.7 REPARIEREN UND AKTUALISIEREN 20
1.8 DEINSTALLIEREN DER PROGRAMME 21
KAPITEL 2. DIE VERWALTUNGSKONSOLE 23
2.1 PROGRAMMHAUPTFENSTER 23
2.2 MIT EINEM REMOTE-COMPUTER VERBINDEN 25
KAPITEL 3. SCHUTZ VOR MALWARE 26
3.1 ALLGEMEINES 26
3.2 REMOTE MALWARE REMOVAL 27
3.3 GRUPPEN-TASKS FÜR MALWARE REMOVAL 29
3.4 VERWALTEN DER TASKS FÜR REMOTE-COMPUTER 31
3.5 QUARANTÄNE 31
3.6 EREIGNISANZEIGE 32
KAPITEL 4. MALWARE SHIELD NUTZEN 35
4.1 MALWARE SHIELD AKTIVIEREN 35
4.2 ACRONIS MALWARE SHIELD KONFIGURIEREN 36
KAPITEL 5. MALWARE-DEFINITIONEN AKTUALISIEREN 42
KAPITEL 6. DER POP-UP-BLOCKER 45
KAPITEL 7. MALWARE-KATEGORIEN 48

Copyright © Acronis, Inc., 2000-2006

Acronis Privacy Expert 9.0 Corporate

Malware (**Mal**icious Soft**ware**) ist eine Technologie, die immer mehr zu einer riesigen Bedrohung für Netzwerke in Unternehmen wird. Versteckte Malware-Programme, die Sie nicht kennen und von deren Existenz Sie nicht wissen, durchdringen Ihr System, sammeln vertrauliche Daten und übermitteln diese über das Netzwerk an unbefugte Personen. Außerdem kann die Leistung im Netzwerk bzw. auf den Netzwerkcomputern so nachlassen, dass die Produktivität der Mitarbeiter sinkt.

Nach den Ergebnissen einer Studie aus dem Januar 2005 sind zwei Drittel aller IT-Manager davon überzeugt, dass die Bedrohung durch Malware an erster Stelle aller Bedrohungen für die Netzwerke steht.

95% der IT-Manager sind außerdem der Meinung, dass zentrales Management der effektivste Weg ist, um eine Anti-Malware-Lösung im Unternehmen einzusetzen.

Acronis hat eine Lösung, die sicherstellt, dass Malware nicht zu einer Bedrohung für Ihre Organisation wird. Acronis Privacy Expert Corporate ist eine zentral gesteuerte Anti-Malware-Lösung, die Ihr Unternehmen vorauswirkend schützt und so die Infektionen durch Malware abwehrt, die vertrauliche Information weitergeben sowie die Netzwerk- und PC-Leistung vermindern könnten.

Das integrierte Programm schützt Netzwerkcomputer bzw. mit dem Internet verbundene Computer. Hauptanliegen der Suite ist es, alle Computer im Netzwerk von den Bedrohungen durch heimlich agierende Malware zu befreien und vorauswirkend vor weiteren Gefährdungen zu bewahren. Mit Hilfe eines Assistenten entfernen Sie vorhandene Malware-Programme (**Malware Removal**), die Funktion **Malware Shield** bietet aktiven Schutz vor neuen Angriffen.

Acronis Privacy Expert Corporate ist aber mehr als nur eine Anti-Malware-Lösung. Das Programm enthält zusätzlich den Acronis Pop-Up-Blocker, ein Tool, das die Aktionen Ihrer Mitarbeiter im Internet gezielt und konfigurierbar von den meisten Werbeeinblendungen und anderen lästigen Erscheinungen beim Surfen mit dem Microsoft Internet Explorer befreit.

Schlüsselfunktionen

Zentrale Funktionen von Acronis Privacy Expert Corporate werden mit der Acronis Privacy Expert Corporate Management Console von einem beliebigen Computer im Netzwerk aus gesteuert und mit Hilfe von Acronis Privacy Expert Corporate Agent auf Remote-Maschinen realisiert. Die folgenden Fähigkeiten von Acronis Privacy Expert Corporate garantieren die Immunität der Netzwerkcomputer.

 Copyright © Acronis, Inc., 2000-2006

Malware entdecken und entfernen

Diese Funktion realisiert das ferngesteuerte Löschen von Malware-Programmen auf Netzwerkcomputern, um zu gewährleisten, dass Außenstehende keinen Zugriff auf interne bzw. vertrauliche Daten erhalten:

- Management der Malware-Tasks auf den Maschinen im Netzwerk von einer zentralen Stelle
- Planmäßige Suche nach Malware auf allen Computern im Netzwerk ohne Benutzereingriff
- Schnelle Prüfung — Suche nach Malware in üblichen Verstecken, einschließlich der Systemordner, Benutzerprofile und der Ordner für temporäre Dateien und in der Windows-Registry
- Tiefenprüfung — Suche nach Malware in ausgewählten Verzeichnissen auf allen Festplatten im System
- Aufspüren von Keyloggern schützt eingegebene Benutzernamen und Kennwörter vor unbefugtem Zugriff
- Eine Quarantäne-Funktion ermöglicht dem Administrator, die Liste der Objekte einzusehen (Dateien, Registry-Keys usw.), die von Malware Removal gelöscht wurden. In dem höchst unwahrscheinlichen Fall, dass das nützlich sein könnte, ist eine Wiederherstellung möglich.

Malware proaktiv abwehren

Acronis Privacy Expert Corporate bietet ein umfassendes Malware Shield, das vor Malware und anderen verdächtigen Programmen schützt, sobald es auf allen im Netzwerk eingebundenen Desktop-Computern und Laptops installiert ist:

- Konstante Systemüberwachung und Warnung über jede verdächtige Aktion unbekannter Programme je nach eingestelltem Schutzgrad
- Automatische Warnung über alle verdächtigen Programme oder Prozesse, die Veränderungen an der Windows-Registry oder an den Startbereichen vornehmen möchten
- Verhindert die Veränderung der Einstellungen von ActiveX-Komponenten

Weitere Funktionen

Die Kernfunktionen von Acronis Privacy Expert Corporate werden durch weitere Features ergänzt.

- Ferngesteuerte Installation der Komponenten von Acronis Privacy Expert Corporate auf Netzwerkcomputern
- Der Acronis Pop-Up-Blocker hindert automatische Pop-Up-Werbefenster während des Surfens im Internet am Erscheinen.

Copyright © Acronis, Inc., 2000-2006

- Acronis Privacy Expert Corporate beinhaltet einen Update-Service für die Datenbank mit den Malware-Definitionen. Dieser Internet-Dienst versetzt Sie in die Lage, die aktuellsten Informationen zum Schutz vor Malware zu erhalten. Dieses Update kann manuell mit Hilfe eines Assistenten erfolgen oder automatisch mit Hilfe eines geplanten Tasks.

Malware Shield und Malware Removal

Kernfunktionen von Acronis Privacy Expert Corporate sind die Entfernung vorhandener Malware (Malware Removal) und der vorbeugende Schutz vor weiteren Bedrohungen durch Malware (Malware Shield).

Acronis Privacy Expert Corporate schützt Sie vor den meisten Bedrohungen, die unter dem Begriff **Malware** zusammengefasst werden. Malware ist ein Kunstwort aus **malicious** (engl. boshaft) und **Software**. Dieser hier verwendete Begriff bezeichnet alle Computerprogramme, die eine offene oder verdeckte Funktion aufweisen, die Ihre Privatsphäre verletzen könnten oder absichtlich mit dem Ziel entwickelt wurden, Schaden anzurichten. Solche möglichen Schadfunktionen sind z.B. Manipulation oder das Löschen von Dateien oder die Unterwanderung der Sicherheitseinrichtungen eines Computers oder die Aufzeichnung von Nutzeraktivitäten und deren Weiterleitung an Dritte.

Beachten Sie, dass Acronis Privacy Expert Corporate auch bei aktivierter Funktion Malware Shield nicht vor jeder Art Malware schützt. Für den Schutz vor Computerviren ist zusätzlich ein spezielles Antivirusprogramm erforderlich.

Als **Malware** werden im üblichen Sprachgebrauch auch Programme bezeichnet, die persönliche Daten des Benutzers ohne dessen Wissen und Zustimmung an den Hersteller der Software oder an Dritte senden. Meist dienen solche Programme dazu, das Verhalten eines Computerbenutzers im Internet zu analysieren, um später beim wiederholten Besuch bestimmter Seiten gezielt Werbebanner oder Pop-Up-Fenster einzublenden, die den Interessen des Benutzers angepasst sind. Die Firmen erhoffen sich davon eine Steigerung der Wirksamkeit dieser Werbemethoden.

Trotz dieser mitunter eindeutigen Absicht, die nicht mit den Wünschen des Benutzers in Einklang steht, ist es rechtlich gesehen nicht ganz ungefährlich, eine Software mit dieser Bezeichnung zu belegen. Ob Sie ein Programm als Malware einstufen oder nicht, ist Ihnen überlassen. In den meisten Fällen haben Sie sogar selbst durch einen Download oder eine Bestätigung den Weg für diese Programme auf Ihren Rechner geebnet. Sie entscheiden also in jedem Fall selbst: Acronis Privacy Expert 9.0 Corporate wird Ihnen die Entscheidung durch die Anzeige **möglicher** Bedrohungen durch Aktivitäten von Programmen erleichtern, die Malware sein **könnten**. Dieser Vorschlag kennzeichnet also immer nur "möglicherweise unerwünschte Software", in der aktuellen Fachliteratur auch **PUS** genannt, **p**otentially **u**nwanted **s**oftware.

 Copyright © Acronis, Inc., 2000-2006

Bei einigen Programmen bzw. Tools sieht die Sache sogar noch ganz anders aus. Es könnte sein, dass Sie als Administrator bewusst ein Programm zur Fernsteuerung eines Remote-Computers installiert haben. Da dieses Tool andererseits aber auch durch Dritte unbemerkt installiert worden sein könnte, wird Acronis Privacy Expert Corporate dieses Programm zunächst als Bedrohung anzeigen. Sie haben dann beim ersten Auftreten die Möglichkeit, solche Programme aus dem Löschzyklus herauszuhalten.

Sollte sich bei der Installation von Acronis Privacy Expert Corporate bereits Software auf Ihrem Rechner befinden, die den beschriebenen Kriterien entspricht, dann können Sie Acronis Privacy Expert Corporate unmittelbar nach der Installation mit der Entfernung beauftragen. Wenn Sie Malware Shield aktivieren, wird diese Funktion dafür sorgen, dass Ihnen von Programmen verursachte, möglicherweise unerwünschte Handlungen gemeldet werden. Bei entsprechender Entscheidung schirmt Malware Shield zukünftig alle weiteren Versuche automatisch ab.

Aus den beschriebenen rechtlichen Gründen stuft Acronis Privacy Expert Corporate Gefährdungen nur als **mögliche** Gefahren ein. Sie müssen dem Malware Shield in der ersten Zeit beibringen, welche Aktivitäten Sie als Gefahr einstufen und deshalb verbieten bzw. welche Aktivitäten Sie zulassen. Beachten Sie, dass Malware Shield bei höchstem Schutzgrad anfangs mitunter Prozesse melden wird, die Sie zulassen oder für die Sie eine permanente Regel erstellen müssen, um die Systemfunktionen und andere gewünschte Aktivitäten sicherzustellen.

Da sich die Zahl der als Malware bezeichneten Programme ständig erhöht bzw. immer weitere Varianten bekannter Software erscheinen, ist der durch Malware Shield gewährleistete Schutz von der Aktualität der verfügbaren Informationen abhängig. Durch tägliche Aktualisierungen der Datenbank mit den Malware-Definitionen sind Sie aber stets auf der sicheren Seite. Diese Aktualisierung können Sie entweder manuell ausführen oder mit einem Zeitplaner automatisieren.

Acronis Privacy Expert Architektur

Acronis Privacy Expert enthält die folgenden Komponenten:

1. **Acronis Privacy Expert Corporate Management Console** — Installation und Management von Acronis Privacy Expert Corporate Agent auf Remote-Maschinen; entfernt Bedrohungen durch Malware auf den Remote-Computern, Planung von Tasks für Malware Removal, Ereignisanzeige durchsuchen u.a.
2. **Acronis Privacy Expert Corporate Agent** — Installation auf den Remote-Systemen, um den Zugriff mit der Acronis Privacy Expert Corporate Management Console zu ermöglichen.
3. **Acronis Malware Shield** — Installation auf den Remote-Systemen, überwacht diese auf verdächtige Anwendungen und Komponenten.

Copyright © Acronis, Inc., 2000-2006

4. **Acronis Pop-Up-Blocker -** Installation auf den Remote-Systemen, wehrt dort unerwünschte Werbefenster beim Surfen im Internet ab.
5. **Acronis License Server** ermöglicht das Management Ihrer Acronis Enterprise Produktlizenzen von einer zentralen Stelle aus. Eine **Acronis License Server Management Console** ermöglicht die bequeme Verwaltung der Lizenzen im **Acronis License Server** über das Netzwerk.

Neues in Acronis Privacy Expert 9.0 Corporate

Acronis Privacy Expert Corporate enthält viele neue und überarbeitete Funktionen. Umsteiger von den Vorversionen von Acronis Privacy Expert Corporate werden wie Neueinsteiger in das Programm neben der überarbeiteten Benutzerschnittstelle und der gesteigerten Performance schnell die Schlüsselfunktionen schätzen:

- Verbesserter Assistent zum Entfernen von Malware (Malware Removal). Enthalten ist eine Funktion zum Aufspüren und Entfernen von Rootkits.
- Neuartiges Malware Shield für den ununterbrochenen Schutz vor Malware in drei möglichen Schutzgraden.
- Täglich aktualisierte Datenbank mit den Malware-Definitionen, die von Acronis Privacy Expert Corporate für die Erkennung und Entfernung von Malware benutzt werden.
- Erweiterter Acronis Pop-Up-Blocker für den Microsoft Internet Explorer, der Einstellungen für den Schutzgrad und die Auswahl der zu blockenden Inhalte bietet.

Nutzungsbedingungen der Software

Die Bedingungen für die Nutzung der Software Acronis Privacy Expert 9.0 Corporate sind in der im Anhang abgedruckten Lizenzvereinbarung beschrieben. Ein Satz einmaliger Seriennummern ist der Nachweis für den legalen Erwerb und die Verwendung einer Komponente von Acronis Privacy Expert 9.0 Corporate. Mit Hilfe von Acronis License Server wird je eine Seriennummer einer Komponente bei deren Installation zugewiesen und das Update der Datenbank mit den Malware-Definitionen für ein Jahr aktiviert. Es wird empfohlen, die Nummer durch Registrierung unter www.acronis.de/registration/ zu personalisieren.

Nach Ablauf der vertraglich festgelegten Zeitspanne ist der Erwerb weiterer Lizenzen erforderlich, um das Abonnement für das Update der Datenbank mit den Malware-Definitionen zu verlängern. Die Komponenten zum Schutz vor Malware können auch ohne Verlängerung des Abonnements für das Update der Datenbank mit den Malware-Definitionen weiterverwendet werden. Allerdings bleibt die Datenbank mit den Malware-Definitionen dann auf dem letzten aktualisierten Stand stehen.

Copyright © Acronis, Inc., 2000-2006

Lizenzpolitik

Die Lizenzierung von Acronis Privacy Expert basiert auf der Anzahl der Workstations, auf denen der Acronis Privacy Expert Corporate Agent installiert wird. Die Anzahl der Installationen von Acronis Privacy Expert Corporate Management Console oder Acronis License Server wird nicht gezählt.

Um die Unternehmenslizenzen zu managen, müssen Sie Acronis License Server installieren und die Lizenzdaten (Seriennummern), die Sie mit Ihrer Kopie von Acronis Privacy Expert erworben haben, dem Server mitteilen (siehe 1.4, »Acronis License Server«). Wenn Sie nachträglich Lizenzen erwerben, dann fügen Sie diese Informationen ebenso hinzu.

Acronis License Server kann mehrere Seriennummern aus einer Textdatei (.txt) importieren, so dass Sie die zeitaufwändige manuelle Eingabe vermeiden können.

Technische Unterstützung (Support)

Nutzer legal erworbener und registrierter Kopien von Acronis Privacy Expert 9.0 Corporate erhalten technische Unterstützung von Acronis. Sie sollten erst versuchen, die Lösung im Benutzerhandbuch zu finden.

Falls Sie Probleme mit der Installation oder Nutzung des Programms haben und diese mit dem Handbuch nicht lösen können oder einfach Fragen haben, besuchen Sie die Acronis-Internetseiten unter der Adresse http://www.acronis.de/support/. Dort finden Sie eine Zusammenstellung der häufig gestellten Fragen (FAQ), in der Sie sehr wahrscheinlich die Lösung Ihres Problems entdecken.

Erst wenn Sie in den FAQ ebenfalls nicht fündig wurden, schicken Sie eine E-Mail an die Adresse support@acronis.de. Dazu benötigen Sie die Registrierungsnummer Ihrer Kopie von Acronis Privacy Expert 9.0 Corporate, die Sie auf der dem Produkt beiliegenden Registrierungskarte finden oder die Ihnen in elektronischer Form übermittelt wurde. Diese geben Sie im Text der Mail an, bevor Sie das Problem beschreiben. Versuchen Sie, das Problem umfassend zu schildern und vergessen Sie nicht, die verwendete Hardware und die Version des Betriebssystems mit anzugeben.

Es wird vorausgesetzt, dass das Betriebssystem durch alle vorhandenen Servicepacks und Patches auf dem neuesten Stand ist, für die verwendete Hardware aktuelle Treiber installiert sind und dass Sie das neueste Build der Software verwenden.

Copyright © Acronis, Inc., 2000-2006

Kapitel 1. Installation

Bei einem Download des Programms erhalten Sie eine ausführbare Programmdatei und eine Anzahl Seriennummern zur Freischaltung der Programmkomponenten. Falls Sie eine Mehrfachlizenz erworben haben, dann erhalten Sie die nötige Anzahl der Seriennummern nach Registrierung auf den Internetseiten von Acronis und Eingabe dieser Seriennummern in elektronischer Form.

Die jeweils aktuellste Version des Handbuchs, die auch die eventuell in neuen Builds (Minor-Updates) hinzugekommenen oder veränderten Funktionen beschreibt, finden Sie im Internet unter http://www.acronis.de/enterprise/download/docs/. Zum Lesen ist eine Version von Adobe Acrobat Reader erforderlich.

1.1 Systemanforderungen und unterstützte Betriebssysteme

Für den Einsatz von Acronis Privacy Expert 9.0 Corporate sind durch die verwendete Hardware folgende Mindestanforderungen zu erfüllen:

- PC-kompatibler Computer mit CPU der Pentiumklasse, 256 MB RAM Arbeitsspeicher,
- Disketten- oder CD-Laufwerk, optionales CD-R/RW-Laufwerk,
- VGA-Monitor, Maus (empfohlen),
- Microsoft Internet Explorer 4.0 oder höher für die korrekte Funktion von Acronis Pop-Up-Blocker

Alle Komponenten von Acronis Privacy Expert Corporate unterstützen die Windows-Betriebssysteme Windows 98/ Me/ NT (einschl. Server)/ Windows 2000 (einschließlich Server und Advanced Server)/ Windows XP und Windows 2003 Server.

1.2 Sicherheitsparameter für Acronis Privacy Expert Corporate einstellen

Acronis Privacy Expert Corporate unterstützt alle Sicherheitsstandards, die in den Server- bzw. den lokalen Versionen von Windows benutzt werden.

- Wenn auf dem Remote-Computer eines der Betriebssysteme Windows NT/2000/XP installiert ist, kann der Acronis Privacy Expert Corporate Agent über die im Netzwerk eingerichteten Sicherheitseinstellungen gesteuert werden. Um einen Remote-Zugriff auf Acronis Privacy Expert Corporate Agent zu erhalten, muss der Benutzer der Acronis Privacy Expert Corporate Management Console Mitglied der Gruppe der Administratoren sein.

 Copyright © Acronis, Inc., 2000-2006

- Auf einem Remote-Computer mit dem Betriebssystem Windows 98/Me müssen Sie während der Installation von Acronis Privacy Expert Corporate Agent einen Benutzernamen samt Kennwort für einen Benutzer eingeben, um den PC später mit der Acronis Privacy Expert Corporate Management Console unter Verwendung dieser Anmeldeinformationen zu steuern.

Einstellungen für die Firewall

Acronis Privacy Expert benutzt die folgenden Ports und IP-Adressen für die Remote-Operationen:

```
SERVER (Acronis Privacy Expert Corporate Agent) UDP PORT: 9876

SERVER (Acronis Privacy Expert Corporate Agent) TCP PORT: 9876, if busy chose PORT AT random

CLIENT (Acronis Privacy Expert Corporate Management Console) UDP PORT: 9877, if busy chose PORT AT random

IPv4 MULTICAST ADDRESS: 239.255.219.45

IPv6 MULTICAST ADDRESS: FF05::fAA5:741E
```

Es könnte sein, dass Sie Einstellungen für eine Firewall präzisieren müssen. Für die in Windows XP Service Pack 2 enthaltene Firewall werden bei der Installation der Komponenten von Acronis Privacy Expert automatische Einstellungen vorgenommen. Stellen Sie aber sicher, dass die Option **Datei- und Druckerfreigabe** in der **Systemsteuerung (Windows-Firewall → Ausnahmen)** auf dem Remote-Computer aktiviert ist, bevor die Remote-Operation beginnt.

1.3 Allgemeine Funktionsweise

Acronis Privacy Expert Corporate arbeitet mit Assistenten und nach einem einfachen Prinzip: Bei allen Aktionen stellen Sie zunächst mit Hilfe des Assistenten eine Handlungsanweisung für Acronis Privacy Expert Corporate zusammen. Mit den üblichen Schaltflächen schreiten Sie z.B. schon während der Installation schrittweise **Weiter** voran, gehen bei Bedarf bereits gewählte Schritte zur Kontrolle bzw. Veränderung **Zurück** oder wählen **Abbrechen**, um den Vorgang nicht auszuführen.

Veränderungen an Datenträgern erfolgen in dieser Phase noch nicht. Durch den Assistenten werden erst Veränderungen vorgenommen, wenn Sie auf **Fertig stellen** klicken. Bis zu diesem Befehl stellt Acronis Privacy Expert Corporate lediglich eine Handlungsfolge zusammen, die Sie bis zur Bestätigung jederzeit ändern oder verwerfen können.

Diese einfache Bedienung der Assistenten wird im gesamten Handbuch vorausgesetzt: Es wird bei der Beschreibung der Abläufe oft nicht ausdrücklich darauf hingewiesen, dass Sie den jeweils nächsten Schritt eines Assistenten mit einem Klick auf die Schaltfläche **Weiter** auslösen müssen.

Copyright © Acronis, Inc., 2000-2006

1.4 Acronis License Server

Vor der Installation von lizenzpflichtigen Komponenten auf dem lokalen oder einem Remote-Computer müssen Sie den Acronis License Server installieren. Der Acronis License Server ist ein Tool für die Verwaltung der Lizenzen, die Sie für die Ausführung eines Acronis-Produkts erworben haben. Dieses Tool müssen Sie entweder lokal auf dem Netzwerk-Computer installieren, von dem aus Sie den (die) anderen Netzwerkcomputer fernsteuern möchten (empfohlen) oder mit Hilfe der zuvor installierten Acronis Privacy Expert Corporate Management Console auf einem beliebigen Computer. Sie können weder Acronis Privacy Expert Corporate Agent noch die anderen lizenzpflichtigen Acronis-Komponenten auf dem lokalen oder einem Remote-Computer benutzen, bis Sie die Seriennummer(n) in den Acronis License Server importiert haben.

Die Lizenzierung von Acronis Privacy Expert Corporate basiert auf der Zahl der Computer, auf denen mindestens Acronis Privacy Expert Corporate Agent, Acronis Pop-Up-Blocker oder Acronis Malware Shield installiert werden. Mit anderen Worten: Sie benötigen eine Lizenz für jeden Computer, auf dem eine der drei Komponenten installiert wird. Sie benötigen z.B. auch dann zwei Lizenzen, wenn Sie auf einem Computer nur das Acronis Malware Shield und auf einer zweiten Maschine nur Acronis Privacy Expert Corporate Agent installieren möchten.

Nicht berücksichtigt wird die Zahl der Installationen von Acronis License Server und Acronis Privacy Expert Corporate Management Console.

Vor der Installation eines Acronis-Produkts mit Acronis License Server müssen Sie den speziellen Acronis License Server dieses Produkts installieren und zwar unabhängig davon, ob bereits der Acronis License Server eines anderen Produkts auf dem gleichen Computer installiert ist. Nach der Installation einer weiteren Variante von Acronis License Server können Sie dann die zugehörigen Seriennummern der unterschiedlichen Produkte mit einer Acronis License Server Management Console verwalten.

Der Acronis License Server muss für die Remote-Computer erreichbar sein. Die Installation von Acronis License Server sollte also auf einem Computer (Server) erfolgen, der die Dienste von Acronis License Server ununterbrochen anbieten kann.

Lokale Installation

Eine lokale Installation von Acronis License Server erfolgt komfortabel durch den Installationsassistenten. Dazu starten Sie die Setup-Datei des erworbenen Produkts auf dem lokalen Computer.

1. Der Begrüßungsbildschirm enthält Befehle für die Installation der Komponenten. Klicken Sie auf den Link von Acronis License Server.

 Copyright © Acronis, Inc., 2000-2006

2. Es erscheint der Endbenutzerlizenzvertrag: Lesen Sie aufmerksam, aktivieren Sie danach die Option **Annehmen** und klicken Sie auf **Weiter**.
3. Wählen Sie die Option **Typisch** und klicken Sie auf **Weiter**. Bei der typischen Installation erfolgt eine lokale Installation von Acronis License Server und Acronis License Server Management Console. Alternativ wählen Sie die Option **Benutzerdefiniert**, um zu entscheiden, welche Komponente lokal installiert wird.
4. Klicken Sie auf Fertig stellen, um Acronis License Server zu installieren.

Acronis License Server remote installieren und verwalten

Falls Sie den Acronis License Server auf einem Remote-Computer installieren möchten, dann wählen Sie den Weg über die Acronis Privacy Expert Corporate Management Console. Starten Sie auf dem Computer, den Sie für die Verwaltung von Acronis Privacy Expert Corporate im Netzwerk verwenden möchten, die Setup-Datei von Acronis Privacy Expert Corporate.

1. Der Begrüßungsbildschirm enthält Befehle für die Installation der Komponenten. Klicken Sie auf den Link von Acronis Privacy Expert Corporate Management Console.
2. Es erscheint der Endbenutzerlizenzvertrag: Lesen Sie aufmerksam, aktivieren Sie danach die Option **Annehmen** und klicken Sie auf **Weiter**.
3. Arbeiten Sie die weiteren Schritte ab und klicken Sie auf **Fertig stellen.**
4. Warten Sie den Installationsvorgang ab.
5. Starten Sie nun die Acronis Privacy Expert Corporate Management Console und klicken Sie auf das Symbol **Installation von Acronis-Komponenten**.
6. Wählen Sie die MSI-Datei von Acronis License Server und klicken Sie auf **Weiter.** Wählen Sie nachfolgend den Computer, auf dem Acronis License Server installiert werden soll.
7. Nach einem Klick auf **Weiter** übergeben Sie die Anmeldeinformationen für den Remote-Computer und entscheiden, ob der Remote-Computer sofort neu starten soll. Falls Sie das zugehörige Kontrollkästchen nicht aktivieren, werden die Veränderungen erst nach einem Neustart des Remote-Computers wirksam.
8. Nach einem Klick auf **Fertig stellen** erfolgt auf dem Remote-Computer eine Installation von Acronis License Server und Acronis License Server Management Console.

Für die Verwaltung von Acronis License Server auf dem Remote-Computer reicht es nun aus, auf einem beliebigen Computer lokal die Acronis License Server Management Console zu installieren. Dazu starten Sie die Setup-Datei des erworbenen Produkts auf dem lokalen Computer.

Copyright © Acronis, Inc., 2000-2006

1. Der Begrüßungsbildschirm enthält Befehle für die Installation der Komponenten. Klicken Sie auf den Link von Acronis License Server.
2. Es erscheint der Endbenutzerlizenzvertrag: Lesen Sie aufmerksam, aktivieren Sie danach die Option **Annehmen** und klicken Sie auf **Weiter**.
3. Wählen Sie die Option **Benutzerdefiniert** und klicken Sie auf **Weiter**.
4. Sorgen Sie dafür, dass nur Acronis License Server Management Console für die Installation vorgemerkt ist, bevor Sie auf **Weiter** klicken.
4. Klicken Sie im abschließenden Schritt auf **Fertig stellen**, um Acronis License Server zu installieren.

Seriennummern in den Acronis License Server importieren

Beim Erwerb des Produkts haben Sie eine oder mehrere Seriennummern zur Lizenzbestätigung erhalten. Sie können diese Seriennummer(n) manuell in den Lizenzserver importieren oder alle gleichzeitig aus einer Datei importieren. Es wird empfohlen, für die Verwaltung der Lizenzen zunächst eine einfache Textdatei anzulegen, in die Sie die erworbenen Lizenzen eintragen. Als Speicherort könnte der Ordner dienen, in dem auch der Lizenzserver gespeichert ist. Falls Sie die Lizenzen per Mail oder in anderer Weise in elektronischer Form erhalten haben, speichern Sie diese als TXT-Datei oder als EML-Datei. Beim Importieren einer Datei im Textformat filtert der Acronis License Server die zugehörigen Serienummern aus dem Text heraus.

Der einfachste Weg zum Import der Seriennummern führt über die Acronis License Server Management Console. Nach der Installation auf einem lokalen Computer finden Sie den Befehl zum Start von Acronis License Server Management Console im Startmenü. Bei der ersten Ausführung müssen Sie eventuell einer aktiven Firewall mitteilen, dass das Programm **LicenseServerConsole** nicht weiter geblockt werden soll. Nach dem Start entscheiden Sie je nach Speicherort von Acronis License Server, ob Sie die Lizenzen auf dem lokalen Computer verwalten möchten oder erst zu einem Computer mit installiertem Acronis License Server verbinden müssen. Für den Import der Lizenzen wählen Sie das Element **Verfügbare Lizenzen verwalten**. Beim ersten Start ist das Fenster leer, da noch keine Lizenzen importiert wurden. Klicken Sie auf **Lizenz hinzufügen** in der Seitenleiste. Es startet der Assistent zum Hinzufügen von Lizenzen. Im zweiten Schritt haben Sie die Wahl, Seriennummern manuell einzutragen und hinzuzufügen oder die Seriennummern aus einer Datei zu importieren. Nach Auswahl dieser Option klicken Sie auf **Durchsuchen** und selektieren die Datei mit den Seriennummern. Nach dem Klick auf **Weiter** sehen Sie die Zusammenfassung: Klicken Sie auf **Fertig stellen**, um den Import zu starten. Nach Abschluss des Imports sehen Sie die Lizenznummern und deren Verwendung. Außerdem finden Sie in der Seitenleiste die Werkzeuge zum Verwalten von verwendeten Lizenzen, zum Hinzufügen weiterer Lizenzen und zum Entfernen von Lizenzen.

 Copyright © Acronis, Inc., 2000-2006

Seriennummern mit dem Acronis License Server Management Tool importieren

Acronis License Server enthält das Kommandozeilentool **LicenseServerCmdLine**.exe, mit dem Sie einen installierten Acronis License Server steuern und die Lizenzen managen. Sie können den Status abfragen, die Lizenzen kontrollieren und weitere Lizenzen hinzufügen.

Nach einer vollständigen Installation von Acronis License Server Management Tool finden Sie die Datei **LicenseServerCmdLine**.exe im Installationsordner, üblicherweise also im Ordner **C:\Programme\Acronis\LicenseServer**.

Zum Ausführen des Programms müssen Sie die Eingabeaufforderung starten (**cmd.exe**) und in dieses Verzeichnis wechseln oder dieses Verzeichnis als Standardpfad definieren, um das Programm zu starten.

Um alle Lizenzen in einem Arbeitsgang zu importieren, benutzen Sie folgenden Befehl:

```
LicenseServerCmdLine --import-file computername filename
```

`computername` – Name des Computers, auf dem der Acronis License Server installiert ist.

`filename` – Name der Datei (*.txt oder *.eml) mit den Seriennummern. Wenn diese Datei im gleichen Verzeichnis wie die Datei LicenseServerCmdLine.exe abgelegt ist, reicht der Dateiname, andernfalls muss der vollständige Pfad angegeben werden.

Beispiele:

```
LicenseServerCmdLine --import-file wsa3456 c:\alsrv\sn.txt
```

```
LicenseServerCmdLine --import-file 192.168.0.163
c:\alsrv\sn.txt
```

```
LicenseServerCmdLine --import-file localhost sn.txt
```

Wenn Sie die Seriennummern manuell importieren möchten, benutzen Sie den Befehl

```
LicenseServerCmdLine --import [computername] [serial1]
[serial2] …
```

`computername` – Name des Computers, auf dem der Acronis License Server installiert ist.

`serial` – Lizenz (Seriennummer)

Beispiele:

```
LicenseServerCmdLine --import 192.168.0.163
AAAAA-BBBBB-CCCCC-DDDDD-EEEEE 2FFFF-3GGGG-4HHHH-IIII5-KKKK6
```

```
LicenseServerCmdLine --import localhost
AAAAA-BBBBB-CCCCC-DDDDD-EEEEE 2FFFF-3GGGG-4HHHH-IIII5-KKKK6
```

```
LicenseServerCmdLine --import MyServer NL6ER-HDVVY-2ZJ27-
RRMMH-AH7Q7
```

Copyright © Acronis, Inc., 2000-2006

LicenseServerCmdLine.exe Referenz

LicenseServerCmdLine.exe benutzt folgende Syntax:

```
LicenseServerCmdLine [option] [parameter1] [parameter2]
```

Optionen und Beispiele für die Benutzung:

```
--list
```

```
LicenseServerCmdLine --list
```

Zeigt eine Liste der aktiven Computer im lokalen Netzwerk, auf denen ein Acronis License Server installiert ist.

```
--status [computername oder IP-Adresse]
```

```
LicenseServerCmdLine --status MyServer
```

```
LicenseServerCmdLine --status 192.168.0.163
```

```
LicenseServerCmdLine --status localhost
```

Zeigt den Status des durch DNS-Computernamen oder die IP-Adresse spezifizierten Computers, auf dem Acronis License Server installiert ist. Falls der Server auf dem lokalen Computer kontrolliert werden soll, kann er auch über localhost angesprochen werden.

Sie sehen zunächst, ob es am angegebenen Ort einen Acronis License Server gibt. Wenn auf dem spezifizierten Computer ein Acronis License Server gefunden wurde, sehen Sie die Zahl der dorthin importieren und die noch verfügbaren Lizenzen.

```
--import [computername] [serial1] [serial2]
```

```
LicenseServerCmdLine --import 192.168.0.163
AAAAA-BBBBB-CCCCC-DDDDD-EEEEE 2FFFF-3GGGG-4HHHH-IIII5-KKKK6
```

```
LicenseServerCmdLine --import localhost
AAAAA-BBBBB-CCCCC-DDDDD-EEEEE 2FFFF-3GGGG-4HHHH-IIII5-KKKK6
```

```
LicenseServerCmdLine --import   MyServer   NL6ER-HDVVY-2ZJ27-
RRMMH-AH7Q7
```

Fügt Informationen über eine neue Lizenz hinzu (neue Seriennummer). Sie können mehr als eine neue Seriennummer importieren, wenn Sie zwischen den einzelnen Seriennummern jeweils ein Leerzeichen schreiben.

```
--import-file [computername] [filename]
```

```
LicenseServerCmdLine --import-file wsa3456 c:\alsrv\sn.txt
```

```
LicenseServerCmdLine --import-file 192.168.0.163
c:\alsrv\sn.txt
```

```
LicenseServerCmdLine --import-file localhost c:\alsrv\sn.eml
```

Importiert die Lizenzen (Seriennummern) aus einer vorbereiteten Textdatei (*.txt, *.eml) auf den spezifizierten Acronis License Server. In der Textdatei stehen die vorhandenen Seriennummern.

 Copyright © Acronis, Inc., 2000-2006

```
--help
LicenseServerCmdLine --help
```

Zeigt einen Hilfetext mit einer Zusammenstellung der Optionen.

1.5 Lokale Installation der Komponenten

Für die Funktionen von Acronis Privacy Expert Corporate ist die Installation von Komponenten erforderlich. Die lokale Installation von Acronis Privacy Expert Corporate ausgewählter Komponenten erfolgt komfortabel durch Installationsassistenten. Dazu starten Sie die Setup-Datei.

Folgen Sie den Anweisungen des Installationsassistenten.

Es ist erforderlich, dass Sie zuerst Acronis License Server installieren und die Seriennummern importieren. Andernfalls werden Sie nicht in der Lage sein, Acronis Privacy Expert Corporate Agent auf den lokalen oder die Remote-Computer zu installieren.

1. Der Begrüßungsbildschirm enthält Befehle für die Installation der Komponenten. Sie haben die Wahl zwischen der lokalen Installation von Acronis Privacy Expert Corporate Management Console, Acronis Privacy Expert Corporate Agent, Acronis Malware Shield, Acronis Pop-Up-Blocker oder Acronis License Server (s. Abb. 1).
2. Nach dem Start einer Installationsvariante erscheint der Endbenutzerlizenzvertrag: Lesen Sie den Lizenzvertrag aufmerksam, aktivieren Sie danach die Option **Annehmen** und klicken Sie auf **Weiter.**
3. Bei der Installation der lizenzgebundenen Komponenten erscheint ein Schritt, bei dem Sie den Acronis License Server für die Überprüfung der Lizenzen spezifizieren müssen. Dieser kann entweder automatisch im lokalen Netzwerk gefunden werden oder manuell angegeben werden. Dazu geben Sie den DNS-Namen des Computer ein, auf dem Acronis License Server installiert ist oder dessen IP-Adresse. Es reicht für die Installation nicht aus, dass der Acronis License Server installiert ist, er muss auch gültige und verfügbare Lizenzen enthalten.
4. Arbeiten Sie die nachfolgenden Schritte des Assistenten ab. Folgen Sie den Anweisungen auf dem Bildschirm.
5. Schließen Sie den Assistenten mit **Fertig stellen.**
6. Zum Abschluss der Installation muss der Computer neu gestartet werden. Bestätigen Sie die entsprechende Abfrage. Alternativ lehnen Sie den sofortigen Neustart ab und installieren zunächst weitere Komponenten.

Wenn Sie bei einer lokalen Installation den Computer erst zu einem späteren Zeitpunkt neu starten können, dann quittieren Sie die Frage nach einem Neustart mit **Nein**. Der Computer wird ohne Beeinträchtigung weiter arbeiten. Beachten Sie aber, dass die Verbindung mit Hilfe einer Acronis Privacy Expert Corporate Management Console zu diesem System erst nach dem Neustart möglich wird.

Copyright © Acronis, Inc., 2000-2006

Abb. 1: Installationsfenster von Acronis Privacy Expert Corporate

Extrahieren der Komponenten

Erfahrene Benutzer können die für eine spätere Installation auf den Remote-Computern benötigten Installationsdateien (MSI-Dateien für die Ausführung mit dem Windows Installer) aus der Setup-Datei von Acronis Privacy Expert Corporate extrahieren. Diese Installationsdateien können auf einem lokalen oder Netzwerklaufwerk abgelegt oder auf einen Wechseldatenträger übertragen werden. Zum Extrahieren der Komponenten sind folgende Schritte nötig:

1. Starten Sie die Setup-Datei.
2. Klicken Sie im Installationsmenü mit der rechten Maustaste auf den Installationslink der Komponente, deren Installationsdatei Sie extrahieren möchten.
3. Im erscheinenden Kontextmenü finden Sie den Befehl **Extrahieren**: Klicken Sie darauf.
4. In der erscheinenden Dateidialogbox geben Sie den Speicherort für die Ablage der extrahierten Dateien an und klicken auf Sie auf **Speichern**.
5. Wiederholen Sie diese Schritte für die anderen Komponenten.

1.6 Acronis-Komponenten auf Remote-Computern installieren

Die Acronis Privacy Expert Corporate Management Console dient der Installation von Acronis-Komponenten auf Remote-Computern, die sich in einem Netzwerk befinden.

 Copyright © Acronis, Inc., 2000-2006

Mit Hilfe der Acronis Privacy Expert Corporate Management Console können Sie folgende Komponenten auf entfernten Computern installieren:

- Acronis Privacy Expert Corporate Agent
- Acronis Malware Shield
- Acronis Privacy Expert License Server
- Acronis Privacy Expert Pop-Up-Blocker

Um eine Komponente auf einem Remote-Computer mit Hilfe der Acronis Privacy Expert Corporate Management Console zu installieren, benötigen Sie auf diesem Computer die Rechte eines Administrators.

Für die Installation von Acronis-Komponenten gehen Sie folgendermaßen vor:

- Installieren Sie die Acronis Privacy Expert Corporate Management Console auf dem lokalen Computer, falls das noch nicht geschehen ist. Starten Sie dann die Acronis Privacy Expert Corporate Management Console.

Klicken Sie auf das Symbol **Installation von Acronis-Komponenten** in der Symbolleiste des Programmhauptfensters der Acronis Privacy Expert Corporate Management Console oder wählen Sie den Befehl **Installation von Acronis-Komponenten** im Hauptmenü **Extras.**

- Im zweiten Schritt des Assistenten wählen Sie die Acronis-Komponente, die Sie installieren möchten (Acronis Privacy Expert Corporate Agent, Acronis License Server, Acronis Pop-Up-Blocker oder Acronis Malware Shield).
- Bei der Installation von Acronis Privacy Expert Corporate Agent, Acronis Pop-Up-Blocker oder Acronis Malware Shield erfolgt die Abfrage des Computers, auf dem der Acronis License Server die Lizenzen verwaltet. Entscheiden Sie, ob Sie den Server automatisch finden lassen oder manuell durch die Angabe des DNS-Computernamens oder der IP-Adresse spezifizieren möchten.
- Wählen Sie einen oder mehrere Computer aus der Liste, auf dem die gewählte Komponente installiert werden soll. Diese Liste zeigt alle Computer, zu denen eine Netzwerkverbindung besteht.
- Nachfolgend müssen Sie den Benutzernamen des Administrators und dessen Kennwort benutzen. **Es wird – auch für die spätere Remote-Verwaltung – angenommen, dass die Konten des Administrators mit gleichem Benutzernamen und Kennwort auf allen ausgewählten Computern existieren**.

Wenn die Remote-Computer die gleichen Anmeldeinformationen verarbeiten können, mit denen Sie auf dem aktuellen Computer angemeldet sind, und die damit verbundenen Rechte auf dem Remote-Computer für eine Installation ausreichen, dann können Sie die Eingabefelder leer lassen.

Copyright © Acronis, Inc., 2000-2006

- Wenn Sie das Kontrollkästchen **Remote-Computer neu starten** auswählen, wird der Remote-Computer automatisch nach der Installation der Komponente neu gestartet. Andernfalls erhalten Sie nach erfolgreichem Abschluss der Installation einen entsprechenden Hinweis im Meldungsfenster, dass die Veränderungen erst nach einem Neustart wirksam werden.
- Klicken Sie auf **Fertig stellen**, um die Komponenten auf den ausgewählten Computern zu installieren.

Die Remote-Installation von Komponenten ist nur auf Computern möglich, die unter Windows NT/2000/XP arbeiten (einschließlich der Server-Versionen). **Computer mit Windows 98/Me erfordern eine lokale Installation der Komponenten**.

Wenn der Remote-Computer das Betriebssystem Windows XP verwendet, muss die (von Windows XP empfohlene) Einstellung **Einfache Dateifreigabe verwenden** unter **Systemsteuerung → Ordneroptionen → Ansicht** deaktiviert sein, bevor Sie mit der Remote-Installation beginnen. Diese Einstellung ist üblicherweise nach einer Standardinstallation aktiviert – Sie sollten also vor einem Installationsversuch diese Einstellung prüfen.

Wenn der Remote-Computer das Betriebssystem Windows XP mit installiertem Service Pack 2 verwendet, muss die Einstellung **Datei- und Druckerfreigabe** unter **Systemsteuerung → Windows-Firewall → Ausnahmen** aktiviert sein, bevor Sie mit der Remote-Installation beginnen.

1.7 Reparieren und aktualisieren

Acronis Privacy Expert Corporate bietet Funktionen für die Reparatur einer beschädigten Installation, das Upgrade auf eine höhere Version und für die Deinstallation. Für diese Aufgaben starten Sie das Installationsprogramm erneut. Wenn Acronis Privacy Expert Corporate eine vorhandene Version im System des Zielcomputers findet, erscheint ein besonderes Assistentenfenster (s. Abb. 2).

 Copyright © Acronis, Inc., 2000-2006

Acronis Privacy Expert Corporate Agent
Ändern, Reparieren oder Entfernen der Installation
Wählen Sie die Operation, die Sie ausführen möchten.
Modifizieren
Ändern der installierten Features.
Reparieren
Stellt den ursprünglichen Zustand der Installation wieder her, ersetzt vermisste oder beschädigte Dateien, Shortcuts und Registrierungseinträge.
Entfernen
Acronis Privacy Expert Corporate von diesem Computer entfernen.
< Zurück
Weiter >
Abbrechen

Abb. 2: Der Assistent für die Reparatur oder die Aktualisierung der Komponenten von Acronis Privacy Expert Corporate

- Mit Auswahl der ersten Schaltfläche modifizieren Sie eine vorhandene Version einer Komponente von Acronis Privacy Expert Corporate. Damit führen Sie den bereits beschriebenen Installationsvorgang erneut aus. Mit Hilfe der windowstypischen Installationselemente wählen Sie, welche Features der zuvor gewählten Komponente installiert werden. Die Schaltfläche ist aber nur aktiv, wenn die zu aktualisierende Komponente aus mehr als einem Feature besteht.
- Die zweite Option ersetzt vermisste oder beschädigte Dateien und stellt so die ursprüngliche Installation wieder her.
- Die dritte Option deinstalliert eine vorhandene Version der Komponente von Acronis Privacy Expert Corporate.

1.8 Deinstallieren der Programme

Sie können jede der lokal installierten Komponenten von Acronis Privacy Expert Corporate separat deinstallieren. Das Entfernen einer Komponente kann alternativ zum oben beschriebenen Verfahren über die Systemsteuerung von Windows lokal auf einem Computer erfolgen.

1. Starten Sie die Windows-Systemsteuerung.
2. Aktivieren Sie den Bereich **Software → Programme ändern oder entfernen**.
3. Markieren Sie die zu entfernende Komponente.

Copyright © Acronis, Inc., 2000-2006

4. Klicken Sie auf **Entfernen**, um die gewählte Komponente zu deinstallieren.

Wenn Sie an dieser Stelle die Schaltfläche **Ändern** wählen, dann gelangen Sie in das in Abb. 2 sichtbare Auswahlmenü, so dass Sie auf diese Weise auch die Installation modifizieren oder reparieren können.

5. Bestätigen Sie die Nachfrage und warten Sie die Vollendung der Handlungen ab.

Auch wenn Sie nicht ausdrücklich darauf hingewiesen werden, sollten Sie den Rechner nach Abschluss der Deinstallation neu starten.

Copyright © Acronis, Inc., 2000-2006

Kapitel 2. Die Verwaltungskonsole

Die Acronis Privacy Expert Corporate Management Console ist das Tool für die Verwaltung der Komponenten auf Remote-Computern, auf denen der Acronis Privacy Expert Corporate Agent installiert ist.

Acronis Privacy Expert Corporate Management Console starten Sie mit dem Befehl **Start → Alle Programme → Acronis → PrivacyExpert → Acronis Privacy Expert Corporate Management Console** oder durch einen Doppelklick auf das bei der Installation angelegte zugehörige Desktop-Symbol.

Acronis Privacy Expert Corporate Management Console ermöglicht folgende Arbeiten:

- Verbindung zu einem Remote-Computer, auf dem der Acronis Privacy Expert Corporate Agent installiert ist.
- Installation, Update oder Deinstallation von Acronis-Komponenten auf den Remote-Computern (erfordert die nötigen Zugriffsrechte).
- Entfernung von Malware und anderen verdächtigen Programmen von den Remote-Computern (Workstations)
- An- bzw. Abschalten von Acronis Malware Shield auf Remote-Computern
- Ereignisanzeige der Operationen von Acronis Privacy Expert Corporate auf einem Remote-Computer einsehen
- Durchsuchen des Quarantäne-Bereichs auf den Remote-Computern und Wiederherstellung eines jeden gelöschten Objekts (Dateien, Registry-Keys usw.), wenn das notwendig ist.

2.1 Programmhauptfenster

Nach dem Start der Acronis Privacy Expert Corporate Management Console erscheint das Programmhauptfenster. Die Programmoberfläche ist in drei Bereiche gegliedert (s. Abb. 3):

Copyright © Acronis, Inc., 2000-2006

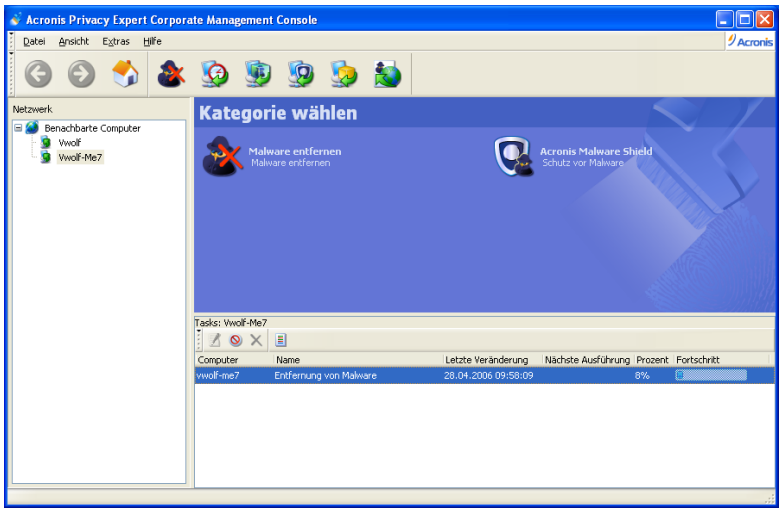

Abb. 3: Acronis Privacy Expert Corporate Management Console Programmhauptfenster

- Im Hauptbereich sehen Sie die verfügbaren Kategorien für ausführbare Operationen. Dort können Sie die Operation wählen, die auf den Remote-Computern ausgeführt werden soll (**Malware entfernen** oder Einstellungen für **Malware Shield**).

Um das System nach Malware zu durchsuchen und gefundene Bedrohungen zu löschen, klicken Sie auf das Symbol **Malware entfernen** im Bereich **Kategorie wählen** des Programmhauptfensters.

Um den automatischen Schutz des Systems vor Malware zu aktivieren, klicken Sie auf das Symbol **Acronis Malware Shield**.

- Um zwischen den Kategorien zu wechseln oder um zum Programmhauptfenster zurückzukehren, benutzen Sie die Schaltflächen **Zurück**, **Weiter** oder **Kategorieauswahl** in der Symbolleiste.
- Der Bereich **Netzwerk** zeigt die Liste der Computer, auf denen ein Acronis Privacy Expert Corporate Agent installiert ist.
- Der unten angeordnete Bereich **Tasks** zeigt den Task-Status für den verbundenen Computer, den Sie im Bereich **Netzwerk** ausgewählt haben. Für aktive Tasks, die gerade ausgeführt werden, ist eine Fortschrittsanzeige sichtbar. Außerdem finden Sie dort die Schaltfläche **Ereignisanzeige**, mit der Sie Informationen über abgeschlossene Remote-Operationen erhalten. Mit der ebenfalls dort angeordneten Schaltfläche **Löschen** können Sie einen zuvor markierten Task löschen.

Copyright © Acronis, Inc., 2000-2006

2.2 Mit einem Remote-Computer verbinden

Sie müssen Ihren Computer mit der Acronis Privacy Expert Corporate Management Console zu einem Computer verbinden, bevor Sie Aktionen mit diesem System ausführen können. Wenn ein Acronis Privacy Expert Corporate Agent auf einem Remote-Computer installiert ist, erscheint dieser Computer in der Liste der Computer im Bereich **Netzwerk**, zu denen Sie mit Hilfe der Acronis Privacy Expert Corporate Management Console eine Verbindung herstellen können.

Falls die Verbindung nicht automatisch hergestellt wird, klicken Sie mit der rechten Maustaste auf einen Computer und wählen dann den Befehl **Verbinden.**

Danach ist die Eingabe von Benutzername und Kennwort für den Zugriff auf die Computer nötig. Es wird aber im Weiteren angenommen, dass Konten mit demselben Benutzernamen und Kennwort auf allen ausgewählten Computern existieren. Andernfalls müssen Sie mit dem zugehörigen Benutzernamen und Kennwort zu jedem Computer einzeln verbinden.

Es wird empfohlen, dass Sie für den Zugriff auf Acronis Privacy Expert Corporate Agent auf allen Computern im Netzwerk ein Administratorkonto mit demselben Benutzernamen und Kennwort anlegen.

Sie verwenden die Acronis Privacy Expert Corporate Management Console auch dazu, den lokalen Computer zu verwalten. Dazu muss auf diesem Computer ebenfalls der Acronis Privacy Expert Corporate Agent installiert sein.

Die erste Handlung nach dem Installieren bzw. den Ausbringen von Acronis Privacy Expert Corporate Agent auf die Netzwerkcomputer sollte das Update der Datenbank mit den Malware-Definitionen sein (siehe Kapitel 5 »Malware-Definitionen aktualisieren«.

Copyright © Acronis, Inc., 2000-2006

Kapitel 3. Schutz vor Malware

Die Entfernung vorhandener Malware (Malware Removal) und der vorbeugende Schutz vor Malware (Malware Shield) sind die Kernfunktionen von Acronis Privacy Expert Corporate.

3.1 Allgemeines

Als **Malware** wird im üblichen Sprachgebrauch ein Programm bezeichnet, das persönliche Daten des Benutzers ohne dessen Wissen oder sogar ohne dessen Zustimmung an den Hersteller der Software oder an Dritte sendet. Es gibt eine Menge solcher Programme, die, wenn sie sich einmal in Ihrem System eingenistet haben, ihre Arbeit von Ihnen unbemerkt ausführen. Jedoch ist anzumerken, dass es auch Programme gibt, die die gleichen Tätigkeiten mit Wissen des Anwenders oder nach bewusster Installation ausüben. In diesem Fall wird Acronis Privacy Expert Corporate diese Programme zwar auch finden bzw. zum Entfernen anbieten, Sie haben es jedoch in der Hand, diese Programme entweder sofort vom Entfernen auszuschließen oder aus der Quarantäne wieder herzustellen. Für weitere Informationen zu den hauptsächlichen Malware-Typen lesen Sie nach im Kapitel 7, »Malware-Kategorien«.

Mit Acronis Privacy Expert werden Sie in die Lage versetzt, Ihre Systeme von Malware zu reinigen und sie vor zukünftigen Beeinträchtigungen zu schützen.

Wie kommt Malware in Systeme von Benutzern?

Am häufigsten gelangt Malware über unbekannte Software in das System, meist mit Freeware oder Shareware. Wenn Benutzer solche Software installieren, dann können anschließend häufig verschiedene Teile des Programms damit beschäftigt sein, vertrauliche Informationen zu sammeln und zu versenden. Das Einblenden lästiger Werbefenster, mit denen eine solche Software üblicherweise finanziert wird, wäre im Vergleich zu anderen Bedrohungen lediglich eine lästige Begleiterscheinung solcher Programme.

Sehr häufig kommen Malware-Programme in als harmlos oder besonders wichtig getarnten E-Mails als Anhang vor und breiten sich aus, sobald ein solcher Anhang geöffnet wird.

Eine andere Quelle von **Malware** sind besuchte Internetseiten. Nicht zuletzt gibt es auch **Malware**, die von kommerziellen Anbietern stammt und die ihr Bestes tut, zusätzliche Informationen zu den Benutzern der Software, zu deren Verhalten und deren Vorlieben zu erfahren.

Unzureichend gesicherte Netze, gemeinsam genutzte Ressourcen und anfällige Programme können arglistige Software dabei unterstützen, einen Computer zu befallen und sich über das Netz auszubreiten.

 Copyright © Acronis, Inc., 2000-2006

Woran ist Malware zu erkennen?

Obwohl Malware üblicherweise im Hintergrund und ohne Wissen des Benutzers funktioniert, gibt es eine Anzahl von Zeichen, die eine solche Tätigkeit vermuten lassen. Wenn Sie diese Zeichen bemerken, sollten Sie Ihre Systeme nach Anwendungen durchsuchen, die im Hintergrund persönliche Informationen ohne Ihr Wissen oder Ihre Zustimmung sammeln und an andere übertragen.

Folgende Escheinungen könnten Anzeichen dafür sein, dass Malware auf einem Computer tätig ist.

- Die Lämpchen für die Anzeige der Tätigkeit der Festplatten blinken, ohne dass ein Programm ausgeführt wird oder ein Dokument geöffnet ist.
- Es werden unbekannte Informationen über das Internet verschickt und empfangen, ohne dass gerade ein Browser oder ein Mailprogramm verwendet wird.
- Die Standardseiten des Internetbrowsers sind häufig verändert
- Wenn mit verschiedenen Programmen gearbeitet oder im Internet gesurft wird, erscheinen Werbeeinblendungen, Pop-Ups und andere Elemente.

Wenn Sie diese Erscheinungen wahrnehmen, sollten Sie Acronis Privacy Expert Corporate damit beauftragen, die Malware zu finden und zu eliminieren, die diese unerlaubten Operationen ausführt. Dazu benutzen Sie den Assistenten zur Entfernung von Malware (Remote Malware Removal).

3.2 Remote Malware Removal

Mit Hilfe von Acronis Privacy Expert Corporate können Sie Malware auf den Computern im Netzwerk finden und gezielt entfernen. Dafür klicken Sie auf die zugehörige Schaltfläche **Malware entfernen** im rechten Teil des Programmhauptfensters.

Im danach erscheinenden Fenster **Malware entfernen** entscheiden Sie, ob Sie **Malware Removal** sofort ausführen, einen Task zur Entfernung von Malware auf Remote-Computern einrichten oder die Datenbank mit den Malware-Definitionen updaten.

Um den Assistenten sofort zu starten, klicken Sie auf den Link **Malware jetzt entfernen.** Nach der Begrüßung durch den Assistenten haben Sie im zweiten Schritt die Möglichkeit, die Computer zu wählen, die nach Malware durchsucht werden sollen. Aktivieren Sie dazu das zugehörige Kontrollkästchen vor den gewünschten Computern oder wählen Sie alle Computer aus, indem Sie das Kontrollkästchen vor **Benachbarte Computer** aktivieren (s. Abb. 4).

Copyright © Acronis, Inc., 2000-2006

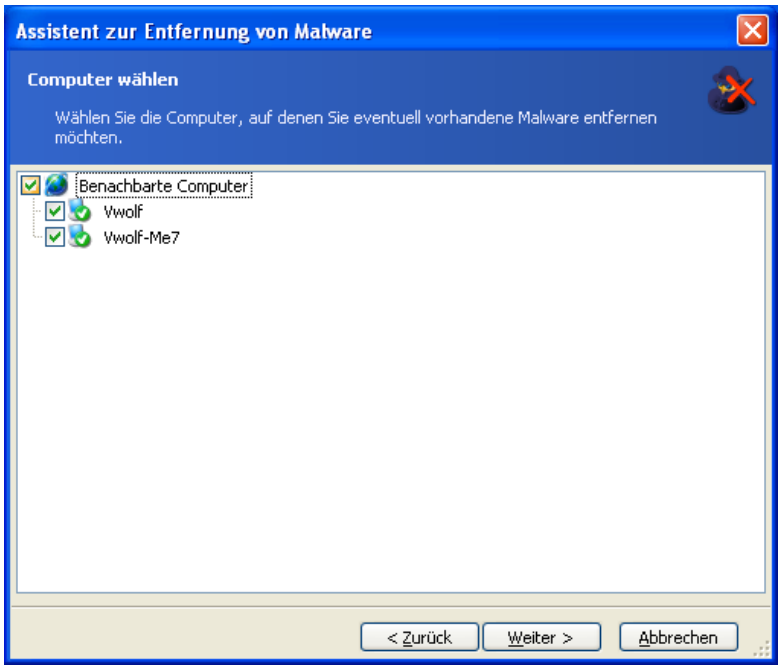

Abb. 4: Auswahl der Computer für die Entfernung von Malware

Der nächste Schritt dient der Einstellung der Intensität, mit der Sie die Suche nach Malware ausführen möchten. Sie haben die Wahl zwischen einer schnellen Prüfung und einer Tiefenprüfung.

- Die Vorgabe **Schnelle Prüfung** ist die Standardeinstellung von Acronis Privacy Expert. In diesem Modus durchsucht Acronis Privacy Expert Corporate nur bekannte Verstecke von Malware im System. Diese Suchmethode ist zu empfehlen, wenn Sie schnelle Resultate benötigen.
- Die alternative **Tiefenprüfung** benutzt eine erweiterte Suchmethode für das Aufspüren von Malware. In dieser Einstellung werden alle lokalen Festplatten nach Malware durchsucht. Je nach Größe der Festplatte(n) dauert diese Methode entsprechend lange.

Im nachfolgenden Schritt entscheiden Sie, ob ein nach der Säuberung eventuell notwendiger Neustart der gewählten Computer sofort ausgeführt werden darf.

Im letzten Schritt des Assistenten sehen Sie das zusammengestellte Script für die Operation zum Entfernen der Malware.

Beachten Sie, dass Malware Removal beim Entfernen der Bedrohungen nur installierte Programme und deren Hinterlassenschaften in den Systemeinstellungen beseitigt. Eventuell vorhandene Installationsprogramme werden dabei nicht entfernt.

Copyright © Acronis, Inc., 2000-2006

3.3 Gruppen-Tasks für Malware Removal

Um die Entfernung von Malware für die Remote-Computer zu automatisieren, können Sie einen Gruppen-Task für Malware Removal anlegen. Dazu klicken Sie auf das Symbol **Task planen** in der Symbolleiste, den Link **Planung der Entfernung von Malware** im Fenster **Malware entfernen** oder wählen den Befehl **Extras → Task planen**.

Im Schritt nach der Begrüßung durch den Assistenten wählen Sie die Computer, für die Sie einen Task planen wollen. Aktivieren Sie dazu das zugehörige Kontrollkästchen vor den gewünschten Computern oder wählen Sie alle Computer aus, indem Sie das Kontrollkästchen vor **Benachbarte Computer** aktivieren.

Der nächste Schritt dient der Einstellung der Intensität, mit der Sie die Suche nach Malware ausführen möchten. Sie haben die Wahl zwischen der schnellen Prüfung und der Tiefenprüfung.

Wenn Sie eine Säuberung zu einem bestimmten Termin aktivieren möchten, dann bestimmen Sie den Startzeitpunkt.

- Nutzen Sie die Option **Täglich**, wenn Sie die Säuberung jeden Tag, an jedem Werktag oder periodisch zu einer bestimmten Zeit automatisch starten möchten.
- Mit der Option **Wöchentlich** realisieren Sie die automatische Säuberung an bestimmten Tagen zu einer festgelegten Zeit. Die dafür einzustellende Periode kann auf spezielle Wochentage und einen Wochenrhythmus festgesetzt werden.
- Die Option **Monatlich** erweitert den planbaren Zeitraum auf bestimmte, monatlich zu wiederholende Aufträge. So geben Sie z.B. eine Tageszahl vor oder den ersten Sonntag im Monat, immer kombiniert mit einer Startzeit.
- Um Tag und Zeit für einen Löschvorgang genau vorzugeben, wählen Sie die Option **Einmalig.**

Alternativ zu einer Säuberung zu einem festen Zeitpunkt bestimmen Sie die Art des Ereignisses, das die Säuberungsaktion startet.

- Soll Acronis Privacy Expert die gewählte Aktion bei jedem Rechnerstart ausführen, dann wählen Sie die Option **Beim Starten des Computers**.
- Soll Acronis Privacy Expert die gewählte Aktion nach jeder Rechnernutzung ausführen, dann wählen Sie die Option **Beim Ausschalten des Computers**.
- Die Optionen **Beim Anmelden** bzw. **Beim Abmelden** nutzen Sie, wenn die gewählte Aktion nur in Verbindung mit einem bestimmten Benutzernamen ausgeführt werden soll. Mit dem zugehörigen Kontrollkästchen können Sie verhindern, dass der Task an einem Tag nicht mehrfach ausgeführt wird.

Copyright © Acronis, Inc., 2000-2006

Um den Task auf Remote-Computern mit dem Betriebssystem Windows NT, 2000, XP oder Server 2003 auszuführen, muss Acronis Privacy Expert den Benutzernamen und das Kennwort des Benutzers kennen (s. Abb. 5).

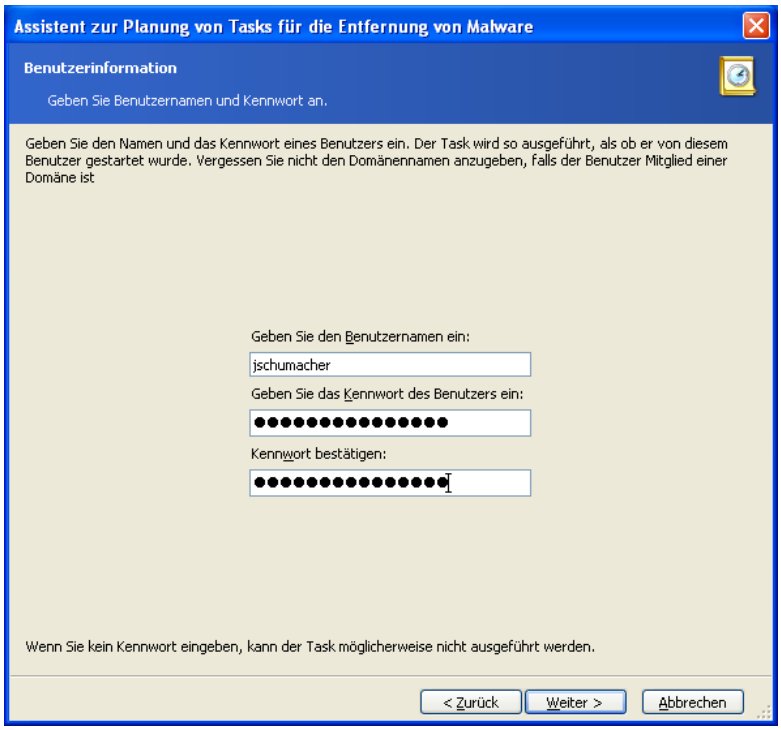
Assistent zur Planung von Tasks für die Entfernung von Malware
Benutzerinformation
Geben Sie Benutzernamen und Kennwort an.
Geben Sie den Namen und das Kennwort eines Benutzers ein. Der Task wird so ausgeführt, als ob er von diesem Benutzer gestartet wurde. Vergessen Sie nicht den Domänennamen anzugeben, falls der Benutzer Mitglied einer Domäne ist
Geben Sie den Benutzernamen ein:
jschumacher
Geben Sie das Kennwort des Benutzers ein:
Kennwort bestätigen:
Wenn Sie kein Kennwort eingeben, kann der Task möglicherweise nicht ausgeführt werden.
< Zurück
Weiter >
Abbrechen

Abb. 5: Eingabe von Benutzernamen und Kennwort

Im oberen Feld geben Sie einen Benutzernamen ein. Geben Sie das Kennwort zweimal in beiden Feldern darunter ein. **Es wird angenommen, dass die Konten des Administrators mit gleichem Benutzernamen und Kennwort auf allen ausgewählten Computern existieren**. Der Task wird auf Computern nicht ausgeführt, die den angegebenen Benutzernamen und das Kennwort nicht akzeptieren. Um sich an einer Windows-Domäne anzumelden, stellen Sie dem Benutzernamen den Namen der Domäne gefolgt von einem Backslash voran (z.B. **domain\benutzer**).

Im nachfolgenden Schritt entscheiden Sie, ob ein nach der Säuberung eventuell notwendiger Neustart der gewählten Computer sofort ausgeführt werden darf.

Mit der Zusammenstellung haben Sie die Task-Planung abgeschlossen. Der Assistent zeigt die Einstellungen im letzten Schritt noch einmal an. Nach dem Klick auf **Fertig stellen** wird der Task auf die gewählten Computer verteilt. Sie erhalten eine Information über den erfolgreichen Abschluss und sehen danach den Task im unteren Bereich des Programmhauptfensters der Acronis Privacy Expert Corporate Management Console. Sie sehen dabei immer die Tasks des Computers, den Sie zuvor im Bereich **Netzwerk** gewählt haben.

Copyright © Acronis, Inc., 2000-2006

Klicken Sie im Bereich **Netzwerk** auf den Eintrag **Benachbarte Computer**, um die geplanten Gruppen-Tasks zu sehen. Durch einen Klick auf **Löschen** können Sie jeweils einen Task für einen Computer löschen

3.4 Verwalten der Tasks für Remote-Computer

Sie können einen beliebigen Task von einem zuvor gewählten Remote-Computer mit den Schaltflächen der Symbolleiste im Task-Bereich verwalten.

- Klicken Sie auf die Schaltfläche **Gewählten Task bearbeiten**, um die Einstellungen für den Task zu verändern.
- Falls ein Task bereits ausgeführt wird, benutzen Sie bei Bedarf die Schaltfläche **Task abbrechen**, um die Ausführung auf dem Remote-Computer abzubrechen.
- Das Löschen eines Tasks auf einem Remote-Computer erfolgt durch einen Klick auf die Schaltfläche **Löschen**.
- Falls Sie im Bereich **Netzwerk** einen einzelnen Computer (nicht **Benachbarte Computer)** gewählt haben, dann ist auch die Schaltfläche Ereignisanzeige aktiv. Nach einem Klick sehen Sie die Historie der auf diesem Computer bereits ausgeführten Tasks.

3.5 Quarantäne

Es könnte mitunter nötig sein, einige der durch die Operationen von Malware Removal gelöschten Elemente (Dateien, Registry-Keys usw.) wiederzuherstellen. Deshalb können Sie die Liste der gelöschten Objekte auf einem Remote-Computer kontrollieren und detaillierte Informationen über die Operationen von Acronis Privacy Expert auf den Remote-Computern erhalten. Um das Durchsuchen und die Wiederherstellung zu gewährleisten, werden gelöschte Elemente in einem Ordner gespeichert, der als Quarantäne dient.

Um die Liste der gelöschten Objekte zu öffnen, klicken Sie auf das Symbol **Quarantäne** in der Symbolleiste oder wählen den Befehl **Extras** → **Quarantäne** im Menü des Programmhauptfensters. Dann wählen Sie einen der verbundenen Computer, um dessen Quarantäne zu sehen.

Sie können immer nur die Quarantäne eines einzelnen Computers sehen. Um den Computer zu wechseln, klicken Sie auf **Zurück** und wählen dann einen anderen Computer.

Im nachfolgenden Fenster sehen Sie eine Liste der Objekte, die auf dem ausgewählten Computer gelöscht wurden. Sie können das Kontrollkästchen vor den gewünschten Objekten aktivieren und diese mit einem Klick auf **Weiter** wieder herstellen (s. Abb. 6).

Copyright © Acronis, Inc., 2000-2006

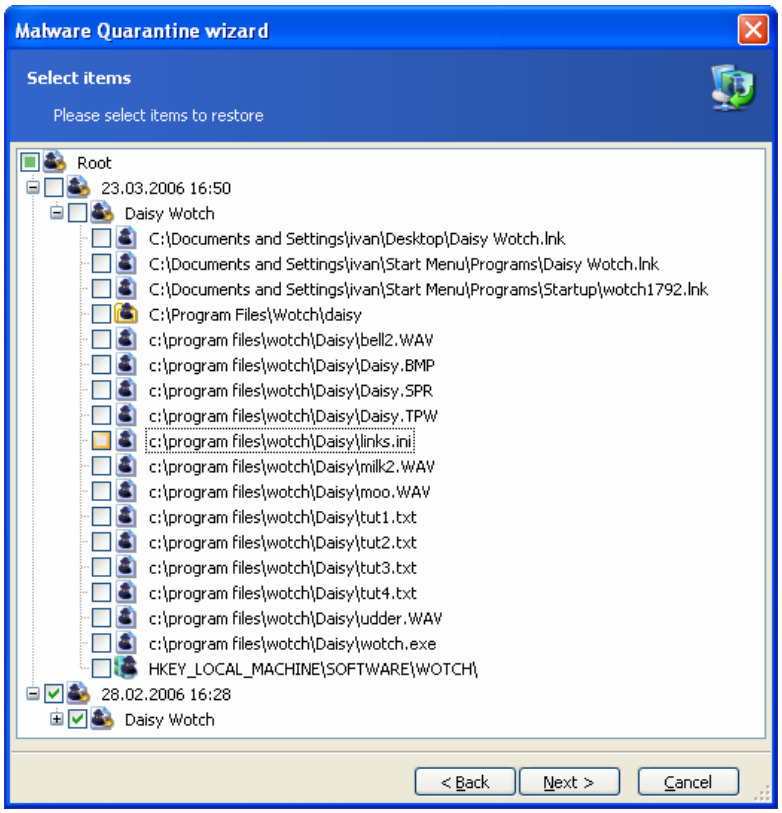

Abb. 6: Quarantäne mit zur Wiederherstellung markierten Elementen

Wenn die Systemkonfiguration geändert worden ist, seit die wiederhergestellten Objekte in Quarantäne gestellt wurden, könnten diese Objekt Konflikte mit der aktuellen Systemkonfiguration auslösen. Deshalb sollten Sie vorsichtig handeln und dieses Feature möglichst nur kurze Zeit nach dem Ausführen von Malware Removal anwenden.

Der Quarantäne-Ordner wird unter **Dokumente und Einstellungen/ [Benutzer]/ Anwendungsdaten/ Acronis/ PrivacyExpert9/ Quarantine** angelegt. Um diesen Ordner zu sehen, muss die Option **Alle Dateien und Ordner anzeigen** bei den **Ordneroptionen** aktiviert sein. In diesem Fall kann der Benutzer den Quarantäne-Ordner auf die übliche Weise mit den Mitteln von Windows löschen.

3.6 Ereignisanzeige

Die Ausführung von Tasks auf den Remote-Computern nimmt einige Zeit in Anspruch und erfolgt meist im Verborgenen. Dann taucht die Frage auf, ob Acronis Privacy Expert die anstehenden Aufgaben erfolgreich erfüllt hat. Für die Kontrolle der Tätigkeit von Acronis Privacy Expert ist die Ereignisanzeige gedacht.

 Copyright © Acronis, Inc., 2000-2006

Diese Anzeige sammelt Informationen über alle Tätigkeiten, die Acronis Privacy Expert Corporate ausgeführt hat. Der Start dieser Anzeige erfolgt mit dem Befehl **Extras → Ereignisanzeige**, einem Klick auf das Symbol oder nach einer Aufforderung von Acronis Privacy Expert im Fehlerfall.

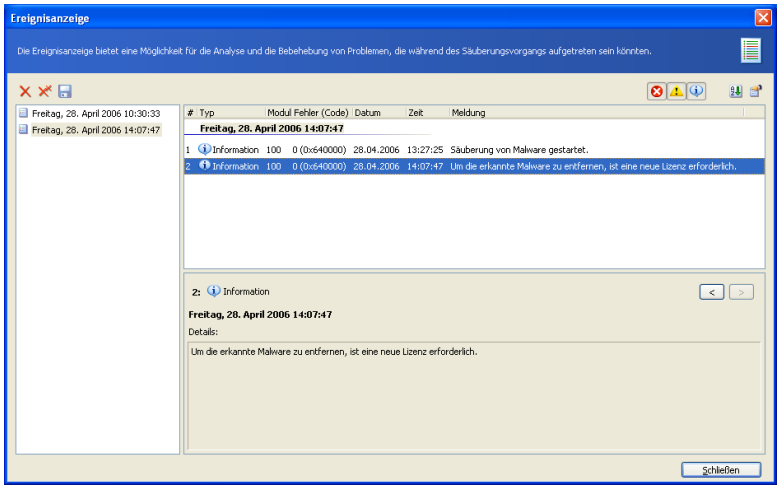
Ereignisanzeige
Die Ereignisanzeige bietet eine Möglichkeit für die Analyse und die Bebehebung von Problemen, die während des Säuberungsvorgangs aufgetreten sein könnten.
Freitag, 28. April 2006 10:30:33
Freitag, 28. April 2006 14:07:47
Typ Modul Fehler (Code) Datum Zeit Meldung
Freitag, 28. April 2006 14:07:47
1 Information 100 0 (0x640000) 28.04.2006 13:27:25 Säuberung von Malware gestartet.
2 Information 100 0 (0x640000) 28.04.2006 14:07:47 Um die erkannte Malware zu entfernen, ist eine neue Lizenz erforderlich.
2: Information
Freitag, 28. April 2006 14:07:47
Details:
Um die erkannte Malware zu entfernen, ist eine neue Lizenz erforderlich.
Schließen

Abb. 7: Die Ereignisanzeige

Das erscheinende Fenster (s. Abb. 7) listet die Aktionen, die von Acronis Privacy Expert Corporate aufgezeichnet wurden. Sie finden Werkzeuge, mit denen Sie die Meldungen sortieren bzw. filtern. Hier finden Sie an nach Auswahl einer Aktion die Detailinformationen von Acronis Privacy Expert Corporate über den Erfolg der einzelnen Handlungen.

Die Ereignisanzeige enthält zwei Bereiche: Der linke Bereich enthält einen Überblick, der rechte Bereich listet die Details eines links ausgewählten Ereignisses auf.

Mit der Ereignisanzeige sind folgende Handlungen möglich:

- **Ereigniseintrag in eine Datei speichern**: Wählen Sie einen Eintrag und klicken Sie auf das Symbol **Ereigniseintrag in Datei speichern**. Nach einem Klick auf das Diskettensymbol öffnet Acronis Privacy Expert Corporate eine Dateidialogbox, mit der Sie die Ereignisse in einer Textdatei speichern können. Acronis Privacy Expert Corporate schlägt einen Dateinamen vor und verwendet innerhalb der Datei XML-Tags für die Darstellung. Wählen Sie den Speicherort und klicken Sie auf **OK**.
- **Gewählten Ereigniseintrag löschen**: Wählen Sie einen Eintrag und klicken Sie auf das Symbol **Ausgewählten Ereigniseintrag löschen**.
- **Alle Ereigniseinträge löschen**: Klicken Sie auf das Symbol **Alle Ereigniseinträge löschen**.

Im rechten Teil des Fensters der Ereignisanzeige sehen Sie die Handlungen von Acronis Privacy Expert Corporate, die zu einem gewählten Eintrag gehören. Sie können diese Liste flexibel gestalten, so dass sie nur die Meldungen eines Typs, ausgewählte Spalten oder eine andere Sortierung anzeigt.

Copyright © Acronis, Inc., 2000-2006

Drei Schaltflächen steuern die Anzeige:

- Das Symbol mit dem weißen Kreuz in einem roten Kreis schaltet die Anzeige der Fehlermeldungen ein bzw. aus.
- Das Symbol mit dem Ausrufezeichen in einem gelben Dreieck schaltet die Anzeige der Warnungen ein bzw. aus.
- Das Symbol mit dem Informationspiktogramm schaltet die Anzeige der Informationen ein bzw. aus.

Um die sichtbaren Spalten zu verändern, klicken Sie entweder mit der rechten Maustaste auf die Spaltenbezeichner oder mit der linken Maustaste auf das Symbol **Wählen Sie die Details** und markieren Sie die Spalten, die Sie sehen möchten.

Um die Meldungen nach einer Spalte zu sortieren, klicken Sie auf den gewünschten Spaltenbezeichner (ein erneuter Klick invertiert die Sortierreihenfolge) oder auf das zweite Symbol von rechts **Sortieren nach** und wählen die gewünschte Spalte.

Außerdem können Sie die Spaltenbreite mit der Maus durch Ziehen verändern.

 Copyright © Acronis, Inc., 2000-2006

Kapitel 4. Malware Shield nutzen

Acronis Privacy Expert ermöglicht nicht nur das Entfernen von bereits vorhandener Malware. Das Programm ist auch dazu in der Lage, den Befall des Systems durch diese Bedrohungen zu verhindern. Diese Funktion wird durch Malware Shield realisiert. Das ist ein spezielles Tool, das Systeme überwacht und dabei verdächtige Programme und Komponenten aufspürt.

4.1 Malware Shield aktivieren

Um Malware Shield auf einem Remote-Computer zu aktivieren, muss es zunächst mit Hilfe von Acronis Privacy Expert Corporate Management Console auf diesem Computer installiert werden.

Das Malware Shield wird während der Remote-Installation von Acronis Malware Shield automatisch aktiviert. Dennoch könnte der Benutzer zwischenzeitlich das Acronis Malware Shield selbstständig ausgeschaltet haben.

Um das Malware Shield auf Remote-Computern zentral zu aktivieren oder zu deaktivieren, wechseln Sie in die Kategorie **Acronis Malware Shield** und klicken auf **Konfiguration der Acronis Malware Shield-Optionen**. Alternativ klicken Sie auf das zugehörige Symbol in der Symbolleiste oder wählen den Befehl **Extras → Konfiguration von Acronis Malware Shield**.

Im zweiten Schritt des Assistenten erscheint die Liste der Computer, auf denen Acronis Privacy Expert Corporate Agent installiert ist. Mit den Kontrollkästchen vor den sichtbaren Computern wählen Sie aus, auf welchen der Computer das Shield aktiviert werden soll.

Falls auf einem der gewählten Computer kein Acronis Malware Shield installiert ist, erhalten Sie zum Abschluss der Aktion eine Fehlermeldung.

Im nächsten Schritt des Assistenten wählen Sie die Option **Acronis Malware Shield aktivieren** (s. **Abb. 8**) bzw. **Acronis Malware Shield deaktivieren**.

Copyright © Acronis, Inc., 2000-2006

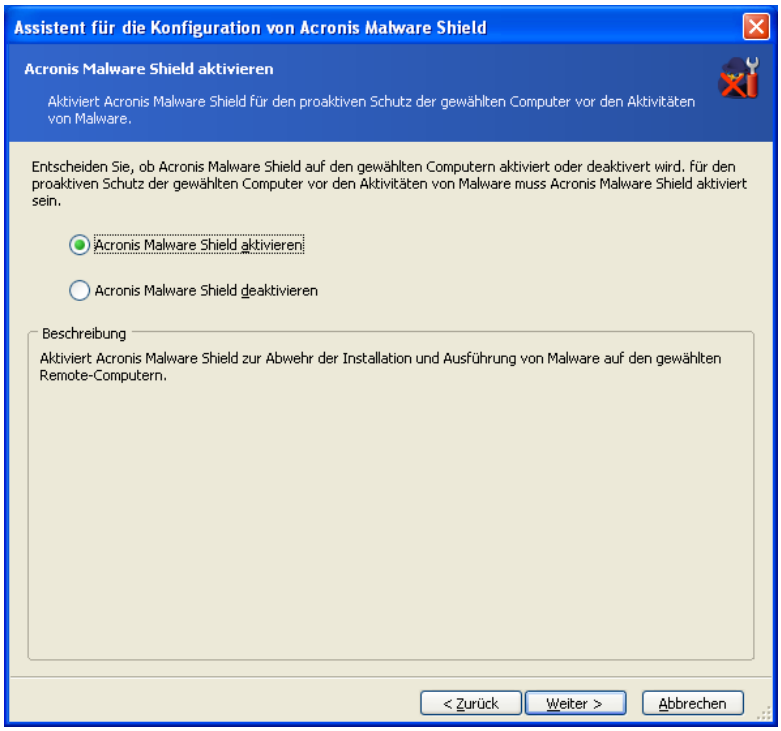
Assistent für die Konfiguration von Acronis Malware Shield
Acronis Malware Shield aktivieren
Aktiviert Acronis Malware Shield für den proaktiven Schutz der gewählten Computer vor den Aktivitäten von Malware.
Entscheiden Sie, ob Acronis Malware Shield auf den gewählten Computern aktiviert oder deaktivert wird. für den proaktiven Schutz der gewählten Computer vor den Aktivitäten von Malware muss Acronis Malware Shield aktiviert sein.
Acronis Malware Shield aktivieren
Acronis Malware Shield deaktivieren
Beschreibung
Aktiviert Acronis Malware Shield zur Abwehr der Installation und Ausführung von Malware auf den gewählten Remote-Computern.
< Zurück
Weiter >
Abbrechen

Abb. 8: Malware Shield auf Remote-Computern aktivieren

Die Zusammenfassung zeigt abschließend noch einmal die Remote-Computer, auf denen die Aktivierung erfolgt. Erst nach einem Klick auf **Fertig stellen** im letzten Schritt des Assistenten erfolgt die Aktivierung von Acronis Malware Shield auf den Remote-Computern. Im Infobereich dieser Computer erscheint das Symbol.

Ein lokal arbeitender Computerbenutzer kann das Acronis Malware Shield komplett stoppen (also auch das Acronis Malware Shield aus dem Speicher entfernen, wenn er mit der rechten Maustaste auf das Symbol im Infobereich der Taskleiste klickt und den Befehl **Beenden** ausführt). Das Symbol von Acronis Malware Shield verschwindet aus der Taskleiste. Ein Neustart von Acronis Malware Shield kann jederzeit wieder mit dem Befehl **Alle Programme → Acronis → Privacy Expert → Acronis Malware Shield** erfolgen.

4.2 Acronis Malware Shield konfigurieren

Ein lokal arbeitender Computerbenutzer kann das Acronis Malware Shield jederzeit durch einen Klick mit der rechten Maustaste auf das Symbol von Acronis Malware Shield im Informationsbereich der Taskleiste von Windows konfigurieren, wenn der Befehl **Acronis Malware Shield Optionen** ausgeführt wird. Damit startet der zuständige Assistent.

Die erscheinende Auswahl (s. Abb. 9) dient dazu, den Schutzgrad einzustellen, mit dem ein aktiviertes Acronis Malware Shield tätig wird.

- Im Schutzgrad **Niedrig**, der als Standard voreingestellt ist, analysiert Acronis Malware Shield die laufenden Prozesse und benachrichtigt nur

 Copyright © Acronis, Inc., 2000-2006

dann, wenn mögliche Bedrohungen auftauchen, die in der Acronis-Datenbank mit den Malware-Definitionen hinterlegt sind. Dieser Schutzgrad ist für die meisten Benutzer empfohlen.

- Im Schutzgrad **Medium** verfolgt Acronis Malware Shield alle gestarteten Prozesse und gibt Alarm, wenn ein Prozess in der Acronis-Datenbank mit den Malware-Definitionen aufgeführt ist. Diese Stufe verhindert Änderungen an den Einstellungen des Web-Browsers, hindert Prozesse daran, sich in den Windows-Startbereich einzunisten, und verhindert die Veränderung der Einstellungen für ActiveX-Komponenten. Bei diesem Schutzgrad erscheinen häufig Meldungen des Alarmfensters, die einen Benutzereingriff erfordern.
- Der sicherste Schutz erfolgt im Schutzgrad **Hoch**. Acronis Malware Shield analysiert alle startenden und laufenden Prozesse und schirmt alle Medien, laufende Prozesse und Windows-Systembereiche ab. In der ersten Zeit muss daher nahezu pausenlos auf das Alarmfenster reagiert werden, bis für alle wichtigen und "normalen" Prozesse eine permanente Regel eingerichtet ist. Dieser Level gibt einen tiefen Einblick in die Arbeit des Rechners und ist nur erfahrenen Nutzern zu empfehlen.

Acronis Malware Shield
Acronis Malware Shield
Bestimmen Sie den Schutzgrad für die Überwachung des Systems auf verdächtige Anwendungen und Komponenten.
Configure Malware Shield
Schutzgrad für das System einstellen:
Schutzgrad
Hoch
Medium
Niedrig
Medium
- Verfolgt alle gestarteten Prozesse und gibt Alarm, wenn ein Prozess in der Acronis-Datenbank der Malware-Definitionen aufgeführt ist.
- Verhindert Änderungen an den Einstellungen des Web-Browsers.
- Hindert Prozesse daran, sich in den Windows-Startbereich einzunisten.
- Verhindert die Veränderung der Einstellungen für ActiveX-Komponenten.
Sie haben keine unaufgelösten Warnungen.
Klicken Sie auf Benutzerdefiniert, um den benutzerdefinierten Schutzgrad einzustellen und die konfigurierten Regeln zu sehen.
Acronis
Compute with confidence
www.acronis.com
OK
Abbrechen
Benutzerdefiniert

Abb. 9: Einstellung des Schutzgrads

Benutzerdefinierte Einstellungen

Zusätzlich zur Einstellung des Schutzgrads können Sie Einstellungen für die Arbeit von Acronis Malware Shield detailliert vornehmen. Dazu klicken Sie auf die Schaltfläche **Benutzerdefiniert** (s. Abb. 9).

Es öffnet sich die Dialogbox **Acronis Malware Shield-Optionen** (s. Abb. 10). Auf der linken Seite sehen Sie die einstellbaren Kategorien, rechts

nach Auswahl einer Kategorie die zugehörigen Steuerelemente. Ein Klick auf **Übernehmen** verändert die Einstellungen sofort, ein Klick auf OK verändert die Einstellungen und schließt die Dialogbox.

- In der Kategorie **Allgemeine Einstellungen** legen Sie fest, ob Acronis Malware Shield bei jedem Start von Windows automatisch ebenfalls startet und ob es aktiviert oder deaktiviert ist.
- In der Kategorie **Prozessanalyse** steuern Sie mit einem Markierfeld, ob das Acronis Malware Shield startende Prozesse analysieren soll. Nur wenn das Kontrollkästchen aktiviert bleibt, kann Acronis Malware Shield vor den Aktivitäten unbekannter oder verdächtiger Programme warnen.

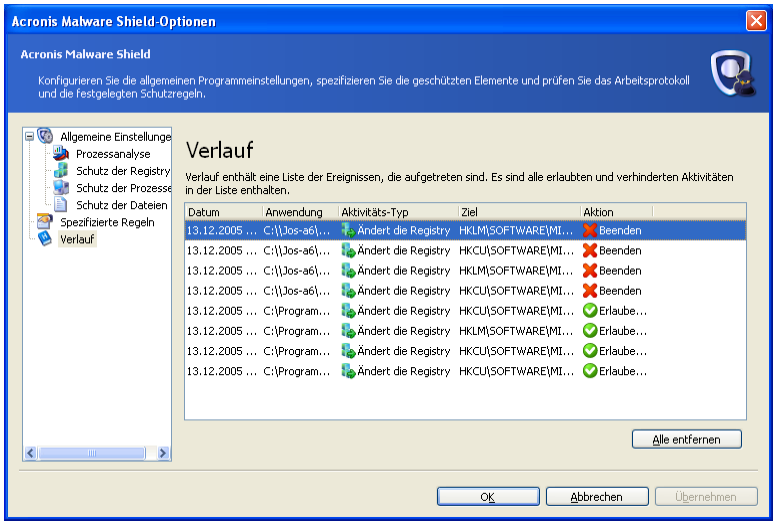
Acronis Malware Shield-Optionen
Acronis Malware Shield
Konfigurieren Sie die allgemeinen Programmeinstellungen, spezifizieren Sie die geschützten Elemente und prüfen Sie das Arbeitsprotokoll und die festgelegten Schutzregeln.
Allgemeine Einstellunge
Prozessanalyse
Schutz der Registry
Schutz der Prozesse
Schutz der Dateien
Spezifizierte Regeln
Verlauf
Verlauf
Verlauf enthält eine Liste der Ereignissen, die aufgetreten sind. Es sind alle erlaubten und verhinderten Aktivitäten in der Liste enthalten.
Datum
Anwendung
Aktivitäts-Typ
Ziel
Aktion
13.12.2005 ... C:\\Jos-a6\... Ändert die Registry HKLM\SOFTWARE\MI... Beenden
13.12.2005 ... C:\\Jos-a6\... Ändert die Registry HKCU\SOFTWARE\MI... Beenden
13.12.2005 ... C:\\Jos-a6\... Ändert die Registry HKLM\SOFTWARE\MI... Beenden
13.12.2005 ... C:\\Jos-a6\... Ändert die Registry HKCU\SOFTWARE\MI... Beenden
13.12.2005 ... C:\Program... Ändert die Registry HKCU\SOFTWARE\MI... Erlaube...
13.12.2005 ... C:\Program... Ändert die Registry HKLM\SOFTWARE\MI... Erlaube...
13.12.2005 ... C:\Program... Ändert die Registry HKCU\SOFTWARE\MI... Erlaube...
13.12.2005 ... C:\Program... Ändert die Registry HKCU\SOFTWARE\MI... Erlaube...
Alle entfernen
OK
Abbrechen
Übernehmen

Abb. 10: Benutzerdefinierte Einstellung von Acronis Malware Shield

- In der Kategorie **Schutz der Registry** treffen Sie Einstellungen, welche Teile der Windows-Registry Sie vor Veränderungen schützen möchten.
  - **Schutz gegen Browser Hijacking** verhindert, dass Malware oder Browser-Plug-Ins Veränderungen an den Vorgaben für die Startseite oder die Suchseite vornehmen.
  - **Schutz gegen Veränderungen der Starteinstellungen** unterbindet ungewollte Veränderungen an den Einstellungen für den Systemstart.
  - **Schutz der Active-X-Konfiguration** sorgt dafür, dass Programme und Prozesse diese Einstellungen nicht unbemerkt ändern, z.B. um arglistigen Code auszuführen.
- Mit Hilfe der Steuerelemente in der Kategorie **Schutz von Prozessen** steuern Sie die Beobachtung aller Programme und Prozesse. Sie können laufende Prozesse vor Eingriffen schützen, den durch Prozesse verwendeten Speicher abschirmen und das Beenden von Prozessen abwehren.

Copyright © Acronis, Inc., 2000-2006

- In der Kategorie **Schutz der Systemdateien** hindern Sie bei aktiviertem Kontrollkästchen Programme daran, Änderungen an kritischen Systemdateien vorzunehmen.
- Die Kategorie **Regeln** enthält eine Liste der permanenten Regeln, die Sie bei der Arbeit mit Acronis Malware Shield spezifiziert haben. Mit Hilfe der Schaltflächen können Sie einzelne oder alle Regeln entfernen.
- Die Kategorie **Verlauf** zeigt alle aufgetretenen Ereignisse und die von Ihnen durchgeführte Aktion (s. Abb. 10).

Nach einem Klick auf **OK** speichert Acronis Privacy Expert Corporate die veränderten Einstellungen. Diese Einstellungen bleiben aktiv, bis Sie den Assistenten erneut ausführen und veränderte Einstellungen speichern.

Das Alarmfenster

Mit Hilfe des so genannten Alarmfensters reagiert Acronis Malware Shield auf Aktivitäten von Programmen, die wichtige Systemeinstellungen verändern möchten. Natürlich wollen das nicht nur solche Programme, die Sie möglicherweise als Malware einstufen. Viele Programme verändern Systemeinstellungen, schreiben wichtige Informationen in die Windows-Registry oder speichern Dateien in Systembereiche von Windows. Jeder Zugriff auf die Computerverwaltung von Windows XP ist schon ein solcher Eingriff (s. Abb. 11). Das Acronis Malware Shield überwacht alle Prozesse, die auf wichtige Systembereiche zugreifen wollen, und überlässt Ihnen die Entscheidung, ob Sie ein gemeldetes Ereignis erlauben, verhindern oder eine Regel erstellen möchten.

Copyright © Acronis, Inc., 2000-2006

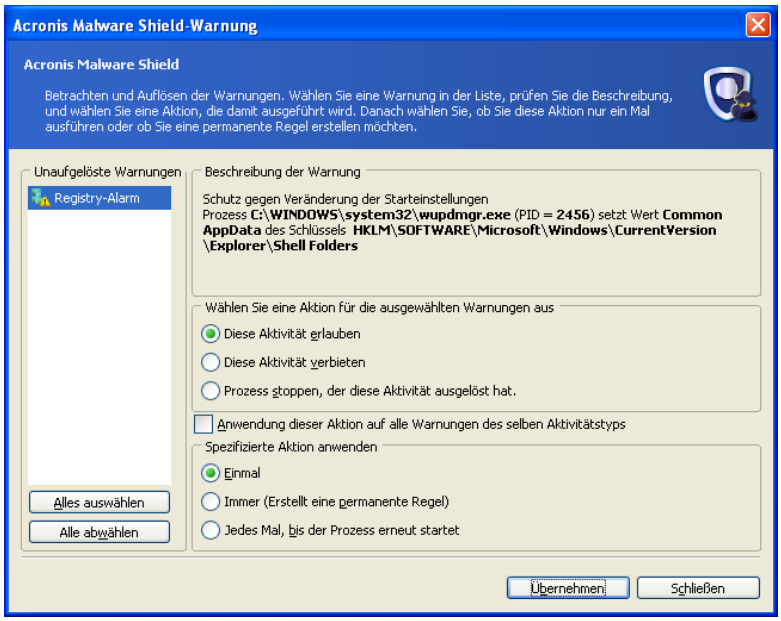
Acronis Malware Shield-Warnung
Acronis Malware Shield
Betrachten und Auflösen der Warnungen. Wählen Sie eine Warnung in der Liste, prüfen Sie die Beschreibung, und wählen Sie eine Aktion, die damit ausgeführt wird. Danach wählen Sie, ob Sie diese Aktion nur ein Mal ausführen oder ob Sie eine permanente Regel erstellen möchten.
Unaufgelöste Warnungen
Registry-Alarm
Alles auswählen
Alle abwählen
Beschreibung der Warnung
Schutz gegen Veränderung der Starteinstellungen
Prozess C:\WINDOWS\system32\wupdmgr.exe (PID = 2456) setzt Wert Common AppData des Schlüssels HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
Wählen Sie eine Aktion für die ausgewählten Warnungen aus
Diese Aktivität erlauben
Diese Aktivität verbieten
Prozess stoppen, der diese Aktivität ausgelöst hat.
Anwendung dieser Aktion auf alle Warnungen des selben Aktivitätstyps
Spezifizierte Aktion anwenden
Einmal
Immer (Erstellt eine permanente Regel)
Jedes Mal, bis der Prozess erneut startet
Übernehmen
Schließen

Abb. 11: Das Acronis Malware Shield blockt eine verdächtige Aktivität

Acronis Malware Shield steuern

An dieser Stelle können Sie das weitere Verhalten von Acronis Malware Shield genauestens steuern. Dazu ist zunächst ein Blick in die technische Information wichtig, die Sie von Acronis Malware Shield erhalten und die im Alarmfenster sichtbar ist. In der Abbildung (s. Abb. 11) versucht ein Prozess mit der PID 2456 einen Wert in die Registrierung von Windows zu schreiben. Auslöser ist das Programm **wupdmgr.exe** – das Windows-Update.

Die Schaltflächen in dieser Ansicht helfen Ihnen nun, die weitere Tätigkeit dieses Prozesses zu steuern:

- Klicken Sie auf **Diese Aktivität erlauben**, wenn Sie dem Prozess genau diese Handlung erlauben möchten.
- Klicken Sie auf **Diese Aktivität verbieten**, wenn Sie dem Prozess genau diese Handlung verbieten möchten.
- Klicken Sie auf P**rozess stoppen, der diese Aktivität ausgelöst hat**, wenn Sie weitere Aktionen dieses Prozesses verhindern möchten.

In diesen Fällen haben Sie nur eine Entscheidung für genau eine Tätigkeit des Prozesses getroffen. Kombinieren Sie deshalb eine dieser Entscheidungen mit dem Kontrollkästchen **Anwendung dieser Aktion auf alle Warnungen des selben Aktivitätstyps**, damit ähnliche Aktivitäten genau so behandelt werden, wie Sie jetzt entscheiden.

Solange die Option im Bereich **Spezifizierte Aktion anwenden** auf **Einmalig** steht, stehen Sie bei diesem Prozess immer wieder vor ähnlichen Entscheidungen. Deshalb können Sie das weitere Verhalten von

 Copyright © Acronis, Inc., 2000-2006

Acronis Malware Shield durch permanente Regeln oder zumindest für diesen Prozess beeinflussen, um zu diesem Fall nicht erneut entscheiden zu müssen.

Nutzen Sie im Kontextmenü des Symbols im Infobereich der Taskleiste von Windows den Befehl **Acronis Malware Shield-Optionen**, um nach einem Klick auf **Benutzerdefiniert** in der Kategorie **Regeln** die spezifizierten Regeln zu kontrollieren und eventuell falsche Entscheidungen zu korrigieren.

Copyright © Acronis, Inc., 2000-2006

Kapitel 5. Malware-Definitionen aktualisieren

Acronis Privacy Expert Corporate bietet für den wirksamen Schutz auch vor den aktuellsten Bedrohungen eine Acronis-Datenbank der Malware-Definitionen. Sie können mit der Funktion **Web-Update** auf die Datenbank zugreifen und täglich die neusten Definitionen downloaden. Eine Lizenz von Acronis Privacy Expert Corporate ermöglicht den Zugriff auf die Acronis-Datenbank für die Dauer eines Jahres. Wenn der Zeitraum abgelaufen ist, können Sie diese Zugriffszeit auf den Webseiten von Acronis durch den Erwerb einer neuen Lizenz erweitern.

Acronis Privacy Expert Corporate enthält einen Assistenten, mit dem Sie die Datenbank mit den Malware-Definitionen für mehrere Remote-Computer gleichzeitig aktualisieren können. Dazu starten Sie die Acronis Privacy Expert Corporate Management Console und starten das Web-Update.

Sie starten den Assistenten für das Remote-Update der Datenbank mit den Malware-Definitionen mit einem Klick auf das Symbol **Web-Updates** oder mit dem Befehl **Extras → Web-Updates.**

Auswahl der Remote-Computer

Im zweiten Schritt des Assistenten erfolgt die Auswahl der Remote-Computer, auf denen die Datenbank mit den Malware-Definitionen aktualisiert werden soll. Es ist sicher sinnvoll, alle sichtbaren Computer zu aktualisieren. Für diesen Fall reicht ein Klick in das Kontrollkästchen vor **Benachbarte Computer**, um alle Remote-Computer zu markieren.

Updatemodus

Anschließend wählen Sie eine Variante zur Ausführung des Updates.

- Mit der Option **Datenbank mit den Malware-Definitionen jetzt aktualisieren** starten Sie den Download der Updates und die nachfolgende Installation auf den Remote-Computern sofort. Im abschließenden Schritt sehen Sie noch einmal die Zusammenfassung mit den zu aktualisierenden Computern, so dass Download und Update nach einem Klick auf **Fertig stellen** sofort beginnen.
- Die zweite Option **Automatisches Update einrichten** stellt einen Task für die gewünschten Remote-Computer zusammen. Dann erfolgen Download und Installation der Updates automatisch. Die Präzisierung erfolgt in den nächsten Schritten.

 Copyright © Acronis, Inc., 2000-2006

Automatisches Update der Datenbank mit den Malware-Definitionen

Wenn Sie im Assistenten die Einstellung automatisches Update gewählt haben, dann erscheinen nach einem Klick auf **Weiter** die Vorgaben für den Startzeitpunkt. Dabei finden Sie folgende Einstellungen:

- Nutzen Sie die Option **Täglich**, wenn Sie das Update der Datenbank mit den Malware-Definitionen jeden Tag, an jedem Werktag oder periodisch zu einer bestimmten Zeit automatisch starten möchten.
- Mit der Option **Wöchentlich** realisieren Sie das Update der Datenbank mit den Malware-Definitionen an bestimmten Tagen zu einer festgelegten Zeit. Die dafür einzustellende Periode kann auf spezielle Wochentage und einen Wochenrhythmus festgesetzt werden.
- Die Option **Monatlich** erweitert den planbaren Zeitraum auf ein bestimmtes, monatlich zu wiederholendes Update der Datenbank mit den Malware-Definitionen. So geben Sie z.B. eine Tageszahl vor oder den ersten Sonntag im Monat, immer kombiniert mit einer Startzeit.

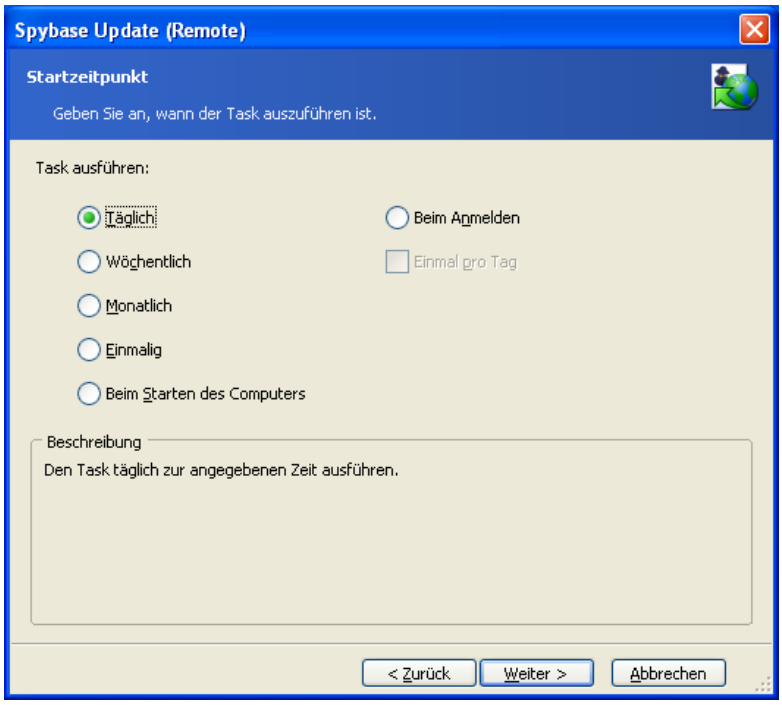

Abb. 12: Zeitplan für das automatische Update einrichten

- Um Tag und Zeit für ein Update der Datenbank mit den Malware-Definitionen genau vorzugeben, wählen Sie die Option **Einmalig.**
- Soll Acronis Privacy Expert das Update der Datenbank mit den Malware-Definitionen bei jedem Rechnerstart ausführen, dann wählen Sie die Option **Beim Starten des Computers**. Mit dem zugehörigen Kontrollkästchen können Sie verhindern, dass der Task an einem Tag mehrfach ausgeführt wird.

Copyright © Acronis, Inc., 2000-2006

- Die Option **Beim Anmelden** nutzen Sie, wenn das Update der Datenbank mit den Malware-Definitionen nur in Verbindung mit einem bestimmten Benutzernamen ausgeführt werden soll. Mit dem zugehörigen Kontrollkästchen können Sie verhindern, dass der Task an einem Tag mehrfach ausgeführt wird.

Den Abschluss der Einrichtung des automatischen Updates der Datenbank mit den Malware-Definitionen bildet die Eingabe des Kennworts eines Benutzers.

Im oberen Feld geben Sie einen Benutzernamen ein. Geben Sie das Kennwort zweimal in beiden Feldern darunter ein. Es wird angenommen, dass die Konten des Administrators mit gleichem Benutzernamen und Kennwort auf allen ausgewählten Computern existieren. Der Task wird auf Computern nicht ausgeführt, die den angegebenen Benutzernamen und das Kennwort nicht akzeptieren. Um sich an einer Windows-Domäne anzumelden, stellen Sie dem Benutzernamen den Namen der Domäne gefolgt von einem Backslash voran (z.B. **domain\benutzer**).

Mit der Zusammenstellung haben Sie die Planung für das automatische Update der Datenbank mit den Malware-Definitionen abgeschlossen. Der Assistent zeigt die Einstellungen im letzten Schritt noch einmal an. Nach dem Klick auf **Fertig stellen** wird der Task auf die gewählten Computer verteilt. Sie sehen danach den Task im unteren Bereich des Programmhauptfensters der Acronis Privacy Expert Corporate Management Console.

 Copyright © Acronis, Inc., 2000-2006

Kapitel 6. Der Pop-Up-Blocker

Beim Surfen im Internet kommt es vor, dass Websites vom User ungewollt weitere Browserfenster starten. Meist enthalten diese Pop-Up-Fenster Werbung oder Verweise auf andere Internetangebote. Das manuelle Schließen dieser Browserfenster ist nicht nur umständlich. Bei zeitabhängigen Internetverbindungen entstehen auch Kosten durch längere Verbindungszeiten und eingeschränkte Bandbreiten. Der Acronis Pop-Up-Blocker von Acronis Privacy Expert hilft Ihnen, diese Pop-Ups beim Surfen mit dem Microsoft Internet Explorer gezielt zu managen.

Um den Acronis Pop-Up-Blocker auf einem Remote-Computer zu installieren, verwenden Sie entweder die Remote-Installation der Acronis Privacy Expert Corporate Management Console oder installieren den Acronis Pop-Up-Blocker lokal mit Hilfe der extrahierten MSI-Datei oder des Installationsprogramms von Acronis Privacy Expert Corporate.

Acronis Pop-Up-Blocker

Der Acronis Pop-Up-Blocker ist automatisch in den Microsoft Internet Explorer integriert und aktiviert, wenn der Computer nach der Installation von Acronis Pop-Up-Blocker neu gestartet wurde. Er verhindert das automatische Öffnen von Fenstern, wenn Sie mit dem Microsoft Internet Explorer eine Webseite besuchen. Ausgenommen sind nur Fenster, die Sie selbst ausdrücklich zugelassen haben. Mit Acronis Pop-Up-Blocker können Sie einen gewählten Web-Content filtern und spezielle Elemente unterdrücken (GIF-Dateien, Flash-Animationen, ActiveX-Objekte, Pop-Ups in Layern usw.).

Um die Einstellungen von Acronis Pop-Up-Blocker für die Zusammenarbeit mit dem Microsoft Internet Explorer zu verändern, haben Sie drei Varianten:

- Klicken Sie auf das Symbol von **Acronis Pop-Up-Blocker** in der Symbolleiste des Microsoft Internet Explorers.
- Benutzen Sie den Befehl **Extras** → **Acronis Pop-Up-Blocker** im Microsoft Internet Explorer.
- Klicken Sie im Microsoft Internet Explorer mit der rechten Maustaste auf eine Seite: Im Kontextmenü finden Sie ebenfalls den Befehl **Acronis Pop-Up-Blocker** mit einem Untermenü zum Deaktivieren bzw. Einstellen der Optionen.

Beim Surfen mit dem Internet Explorer informiert **Acronis Pop-Up-Blocker** mit Meldungen in der Statusleiste des Microsoft Internet Explorers über die Tätigkeit.

Für die korrekte Funktion sollten Sie den in den neueren Versionen von Microsoft Internet Explorer enthaltenen Microsoft Popupblocker mit dem Befehl im Menü **Extras** deaktivieren.

Copyright © Acronis, Inc., 2000-2006

Generelle Einstellungen

Nach dem Start des Assistenten für die Einstellung der Acronis Pop-Up-Blocker-Optionen können Sie die Arbeitsweise dieses Werkzeugs Ihren Bedürfnissen anpassen.

In den Grundeinstellungen verändern Sie die Funktionsweise:

- Mit den zugehörigen Kontrollkästchen (s. Abb. 13) aktivieren oder deaktivieren Sie den Pop-Up-Blocker von Acronis Privacy Expert Corporate.

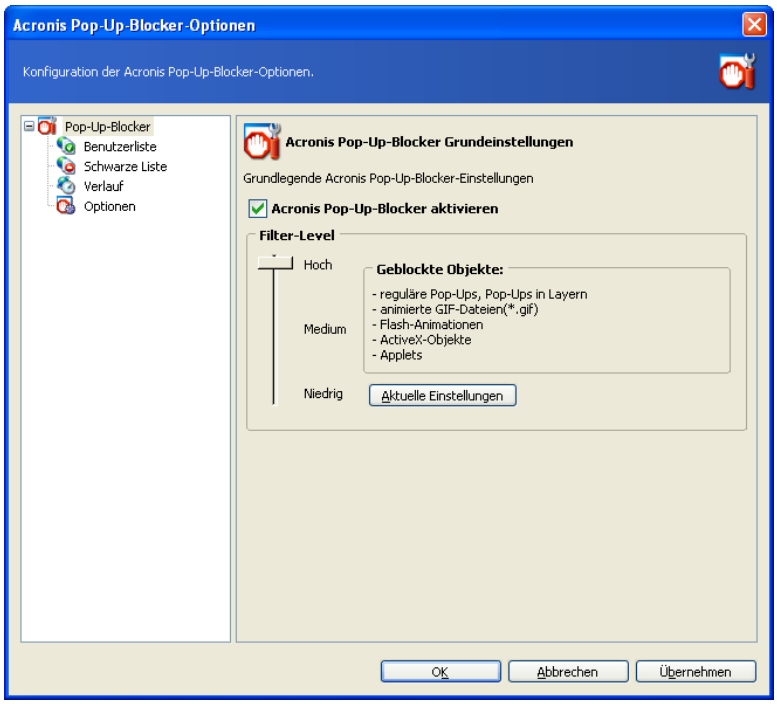

Abb. 13: Die Einstellungen für Acronis Pop-Up-Blocker

- Mit dem Schieber wählen Sie zwischen drei vorgegebenen Filter-Leveln aus, welche Objekte Acronis Pop-Up-Blocker blocken soll. Die Beschreibung rechts neben dem Schieber gibt Auskunft, welche Objekte in den Standardstufen geblockt werden. Bei aktiviertem Acronis Pop-Up-Blocker werden nur reguläre Pop-Up-Fenster geblockt.
- Nach einem Klick auf **Aktuelle Einstellungen** können Sie die Vorgabe der Level verändern: Sie können mit zugehörigen Kontrollkästchen das Blocken von Objekten zu- oder abschalten.

Weitere Einstellungen nehmen Sie in den untergeordneten Zweigen des Einstellungseditors vor:

- Der Zweig **Verlauf** ist eine exakte Darstellung der Browseraktivitäten. In der Liste können Sie Webseiten markieren und sie entweder auf die **Benutzerliste** oder auf die **Schwarze Liste** setzen. Pop-Ups von Seiten

Copyright © Acronis, Inc., 2000-2006

auf der schwarzen Liste werden nach Bestätigung der Veränderungen geblockt, Pop-Ups von Seiten auf der weißen Liste zugelassen.

- Im Zweig **Optionen** steuern Sie weitere Einstellungen, z.B. den Umgang von **Acronis Pop-Up-Blocker** mit erscheinenden Fenstern und Dialogboxen, die Art der Benachrichtigung und die Tastenkombination, mit der Sie den **Acronis Pop-Up-Blocker** zeitweilig außer Kraft setzen.

Benutzerliste

Wenn Sie für eine spezielle Webseite manuell Pop-Ups zulassen möchten, nehmen Sie diese in die Benutzerliste auf. Das ist die Liste der Seiten, für die Sie spezielle Einstellungen treffen wollen. Die Zuordnung zu dieser Liste erfolgt durch Auswahl der Adresse im Zweig **Verlauf**. Aber auch im Zweig **Schwarze Liste** finden Sie für diesen Zweck die Schaltfläche **Verschieben in Benutzerliste**.

- Durch einen Klick auf die Schaltfläche **Hinzufügen** und anschließende manuelle Eingabe der URL nehmen Sie eine Website in diese Liste auf. Dabei können Sie festlegen, wie die Objekte der Seite behandelt werden sollen.
- Die Verwaltung erfolgt über die Schaltflächen **Verschieben in Schwarze Liste**, **Bearbeiten** bzw. **Entfernen**.
- Durch einen einzigen Klick auf **Leeren** entfernen Sie alle Einträge auf der Liste.

Schwarze Sites

Sie können den Acronis Pop-Up-Blocker auch benutzen, um eine komplette Webseite zu blockieren. Dazu setzen Sie die zugehörige URL auf die **Schwarze Liste**. Falls dann der Versuch unternommen wird, auf eine solche Seite zuzugreifen, unterbindet Acronis Privacy Expert den Zugriff und informiert durch eine Nachricht darüber, dass sich die URL auf der schwarzen Liste befindet.

Copyright © Acronis, Inc., 2000-2006

Kapitel 7. Malware-Kategorien

Das abschließende Kapitel enthält ergänzende Informationen über verbreitete Malware und Malware-Parasiten. Acronis Privacy Expert Corporate schützt Sie vor den meisten dieser Bedrohungen. Zusammengefasst werden solche Bedrohungen oft mit dem Begriff **Malware**. Malware ist ein Kunstwort aus **malicious** (engl. boshaft) und **Software**. Dieser Überbegriff bezeichnet alle Computerprogramme, die eine offene oder verdeckte Schadfunktion aufweisen und absichtlich mit dem Ziel entwickelt werden, Schaden anzurichten. Solche Schadfunktionen sind z.B. Manipulation oder das Löschen von Dateien oder die Unterwanderung der Sicherheitseinrichtungen eines Computers.

Beachten Sie, dass Acronis Privacy Expert Corporate auch bei aktivierter Funktion Acronis Malware Shield nicht vor jeder Art Malware schützt. Für den Schutz vor Computerviren ist ein spezielles Antivirusprogramm erforderlich.

Adware

Eine Art des Marketings unter Ausnutzung des Internets über Banner in Freeware und Shareware. Oft werden die Banner beim Ausführen des Programms aus dem Internet geladen, was den Datenverkehr steigert und Internetverbindung ausbremst. Der Begriff **Adware** ist ein Kunstwort aus den englischen Begriffen **advertising**, Werbung, und **software**, Programm. Er steht üblicherweise für kostenlose und funktionell uneingeschränkte Software, die dem Benutzer zusätzlich zur eigentlichen Funktionalität des Programms Werbebanner oder Werbe-Pop-Ups zeigt. Diese Werbeeinblendungen sind oft nicht abschaltbar. Der Hersteller der Software, die meist als Freeware kostenlos vertrieben wird, finanziert durch den Verkauf von Werbeeinblendungen Dritter seine Leistungen. Bei vielen Programmen im Sharewarebereich ist es möglich, gegen Bezahlung eine werbefreie Vollversion zu erhalten bzw. die enthaltene Werbung abzuschalten. Das Anzeigen von Werbung durch normale Adware und das Auswerten von Benutzerdaten durch Spyware haben eigentlich nichts Gemeinsames. Da es aber viele Programme gibt, die Adware und Spyware gleichzeitig sind, wird Adware oft mit Spyware gleichgesetzt.

Browser Helper Objects

Browser Helper Objects (Browserhilfsobjekte) sind Zusätze für den Browser und werden oft einfach BHO genannt. Ein Browserhilfsobjekt ist ein kleines Programm, das die Funktionalität des Internet Explorers erweitert. Einige Browserhilfsprogramme sind wirklich nützlich: Beispiele dafür sind zusätzliche Symbolleisten im Internet Explorer, aber auch versteckte Funktionen wie z.B. die Tools von Adobe zum Anzeigen von PDF-Dateien im Internet Explorer. Aber es gibt andere Browserhilfsobjek-

 Copyright © Acronis, Inc., 2000-2006

te, die ohne Ihre Erlaubnis Informationen über Ihre Surfgewohnheiten sammeln oder für andere arglistige Zwecke verwendet werden können. Über die Bedrohung Ihrer Privatsphäre hinaus können Unverträglichkeiten mit dem System Gefahren für die Systemstabilität auslösen. Adware und Spyware, aber auch Hijacker benutzen Browserhilfsobjekte oft, um Werbung zu zeigen oder das Surfverhalten zu protokollieren, da ein Browserhilfsobjekt Zugriff auf die Adresse jeder besuchten Seite hat und diese auch umleiten kann.

Browser-Hijacker

Browser-Hijacker (Entführer) sind kleine Programme, mit denen die Einstellungen des Browsers manipuliert werden. Diese Programme leiten Seitenaufrufe und Suchanfragen auf bestimmte Seiten um. Browser-Hijacker haben die Fähigkeit, Ihre Netzsuchen durch die Suchmaschinen der Hersteller zu ersetzen, verschriebene oder unvollständige URLs umzuleiten und die im Internet Explorer eingestellte Startseite zu ändern. Ziel der Umleitungen sind oft kostenpflichtige Suchseiten oder Seiten mit pornografischem Inhalt. Browser-Hijacker gehören zur Kategorie der so genannten Malware, die sich meist ohne Wissen des Benutzers im Hintergrund installiert und dabei oft Sicherheitslücken in der Browsersoftware ausnutzt.

Betroffen von diesen Schädlingen sind zurzeit fast ausschließlich die Benutzer des Microsoft Internet Explorers.

Kommerzielle Keylogger

Keylogger registrieren, welche Tasten der Benutzer eines Computers benutzt und versenden diese Information häufig per E-Mail. Oft können solche Applikationen auch die Zeit speichern, zu der Programme geöffnet oder geschlossen werden. Üblicherweise sind solche Programme ohne Wissen des Benutzers auf dem Computer tätig.

Keylogger werden oft von Hackern verwendet, um vertrauliche Daten wie Benutzernamen und Kennwörter auszuspähen. Die von Acronis Privacy Expert Corporate erfassten Software-Keylogger schalten sich zwischen Betriebssystem und Tastatur, um die Eingaben erst zu lesen und dann an das Betriebssystem weiterzugeben. Manche Keylogger speichern die Eingaben auf der Festplatte des überwachten Rechners, andere senden sie über das Internet an einen anderen Computer.

Dialer

Oft werden auch **Dialer** (Einwahlprogramme auf Telefon-Mehrwertrufnummern) zur Malware gezählt, obwohl sie das grundsätzlich nicht sind. Einwahlprogramme sind dann nützlich, wenn sie bewusst zur Verbindungsherstellung mit dem Internet benutzt werden. Die so genannten DFÜ-Verbindungen (Dial-up Networking, Einwahlverbindung),

Copyright © Acronis, Inc., 2000-2006

die für die Verbindung zum Internetprovider genutzt werden, sind im weitesten Sinne ebenfalls Dialer.

In diesem Zusammenhang gemeint sind illegale Dialer-Programme, die eine normale Verbindung heimlich austauschen. Sie spionieren Sie nicht aus, können Ihnen aber finanziellen Schaden zufügen, da sie meist auf sehr teure Verbindungen umschalten. Illegale Dialer haben die Fähigkeit, im Hintergrund zu laufen und ihre Gegenwart zu verbergen.

Exploit/Sicherheitslöcher

Ein **Exploit** (engl. to exploit - ausnutzen) ist ein Computerprogramm, das spezifische Schwächen, Sicherheitslöcher oder Fehlfunktionen eines anderen Computerprogramms ausnutzt, häufig mit destruktiver Absicht. Exploits können beim Öffnen von augenscheinlich völlig harmlosen Dateien, z.B. Bilddateien, aktiviert werden, indem den Bilddateien Maschinencode beigefügt ist und die Datei in einer Weise manipuliert wurde, dass dieser Maschinencode ausgeführt wird. Eine aktive Form von Exploits sind Angriffe aus dem Internet mit Hilfe manipulierter Datenpakete auf Schwachstellen in der Netzwerksoftware. Oft werden auf diesem Weg Tools installiert, die einem Angreifer Zugriffe auf den Rechner gestatten.

Fernsteuerung

Remote Access Tools (RAT), Fernsteuerung: eigentlich ein Programm für die Fernwartung von Computern, das in Netzwerken nicht unüblich ist. So kann z.B. der Support in einem Firmennetzwerk die Kontrolle über einen fehlerhaften Rechner übernehmen und eine Reparatur ausführen, ohne dass der Computer aufgesucht werden muss. In einigen Fällen könnten Benutzer nicht von der Tätigkeit solcher Anwendungen wissen.

Rootkit

Rootkit (sinngemäß Baukasten für den Administrator/Root) ist ein Begriff für Programme, die nach dem Eindringen in ein Computersystem installiert werden, um das Eindringen zu verbergen, Prozesse zu verstecken, Daten zu kopieren und Tastatureingaben aufzuzeichnen. Ursprünglich aus der UNIX/LINUX-Welt stammend wird der Begriff auch auf Programme übertragen, die ihre Tätigkeit auch ohne Anmeldung als Administrator verrichten. Dabei werden die Tarnfunktionen dieser Programme vor allem benutzt, um die Tätigkeit eines „Einbrechers" vor Antivirensoftware zu verstecken.

Sniffer

Sniffer (Schnüffler) sind Programme, die den Verkehr im Netzwerk beobachten (gesendete und empfangene Datenpakete). Sniffer können eine ernste Bedrohung darstellen, da sie in der Lage sind, Benutzerna-

 Copyright © Acronis, Inc., 2000-2006

men, Kennwörter und private Information zu erfassen und zu entschlüsseln. Die meisten Protokolle (FTP, POP, HTTP, Telnet) übermitteln vertrauliche Informationen unverschlüsselt, so dass ein Eindringling leicht Zugriff auf Informationen erhalten kann, wenn er Sniffer-Filter aufstellt und darauf wartet, dass sich das Opfer beim Server meldet. Außerdem könnten Sniffer den normalen Betrieb von Computern und Netzwerk empfindlich stören.

Spyware

Als **Spyware** wird im üblichen Sprachgebrauch ein Programm bezeichnet, das persönliche Daten des Benutzers ohne dessen Wissen bzw. ohne dessen Zustimmung an den Hersteller der Software oder an Dritte sendet. Oft wird solche Spyware verwendet, um "kostenlose" Produkte anzubieten. Meist dienen die Spyware-Programme dazu, das Verhalten eines Computerbenutzers im Internet zu analysieren, um später beim wiederholten Besuch bestimmter Seiten gezielt Werbebanner oder Pop-Up-Fenster einzublenden, die den Interessen des Benutzers angepasst sind.

Toolbars

Toolbars machen die Benutzung eines Browsers angenehmer, wenn sie nach einem Download installiert werden. Beispiele für nützliche Toolbars (Werkzeugleisten) sind die Leisten von Google, Alexa und Yahoo. Obwohl sie sehr praktisch sind, haben diese Taskleisten die Fähigkeit, alles zu verfolgen, was Sie im Internet tun, und diese Information an den Anbieter zu übermitteln. Es ist sinnvoll, vor dem Download und der Installation einer solchen Toolbar die Nutzungsbedingungen und die Datenschutzbestimmungen der Anbieter zu lesen.

Trojaner

Ein Trojanisches Pferd (kurz Trojaner) ist eine Kombination eines (manchmal nur scheinbar) nützlichen Wirtsprogramms mit einem versteckt arbeitenden, bösartigen Teil, oft Spyware oder Backdoor. Ein Trojanisches Pferd verbreitet sich nicht selbst, sondern wirbt mit der Nützlichkeit des Wirtsprogramms für seine Installation durch den Benutzer.

Copyright © Acronis, Inc., 2000-2006

Stichwortverzeichnis

A

Acronis License Server 12
  mehrere Produkte 12
Acronis License Server Management Console. 13
Acronis Privacy Expert Corporate
  Installieren 17
Acronis Privacy Expert Corporate
  Reparieren 20
Acronis Privacy Expert Corporate
  Aktualisieren 20
Administratorkonto 25
Adware **48**
Antivirusprogramm **6**, **48**
Assistenten **11**
Aufgaben kontrollieren 32
Automatisches Update 43

B

Benachbarte Computer 27
Benutzerliste 47
Betriebssysteme 10
BHO 48
Browser Helper Objects 48
Browser-Hijacker **49**
Browserhilfsobjekte 48

C

Computer verbinden 25

D

DFÜ-Verbindungen 49
Dialer **49**

E

Endbenutzerlizenzvertrag 17
Ereignisanzeige 24, 32, **33**
Exploit **50**
Extras
  Ereignisanzeige 33
  Quarantäne 31
  Web-Updates 42

F

FAQ 9
Fernsteuerung **50**
Funktionsweise 11

G

Gruppen-Tasks 29

I

Installation 17
Installation der Management Konsole 23
Installation von Acronis Komponenten 19
Installationsassistent 17

K

Keylogger **49**
Komponenten auf Remote-Computern installieren 18

L

Liste der gelöschten Objekte 31

M

Malware **6**, **26**, **48**
Malware entfernen 27
Malware entfernen 24
Malware Removal 27
Malware Shield konfigurieren 36
Malware Shield Optionen 36
Management Konsole
  Malware entfernen 24
  Programmhauptfenster 23
Management-Konsole 23
Mangement Konsole
  Operation wählen 24
Mehrwertrufnummern 49

N

Nutzungsbedingungen 8

P

Pop-Up-Blocker **45**
Programmhauptfenster Management Konsole 23
PUS 6

Q

Quarantäne 5, 31, 32

R

RAT 50
Remote Access Tools **50**
Remote-Computer verwalten 23
Remote-Operationen kontrollieren 24
Rootkit **50**

S

Schnelle Prüfung 28
Schwarze Sites 47
Sniffer **50**
Software-Keylogger 49
Spybase
  Automatisches Update 42
Startzeitpunkt 29
Support 9
Systemanforderungen 10

T

Task planen 29
Task-Status 24
Technische Unterstützung 9
Tiefenprüfung 28
Toolbars **51**
Trojaner **51**
Trojanisches Pferd **51**

U

Unterstützte Betriebssysteme 10
Update **7**

V

Verbinden zum Remote-Computer 25

W

Windows-Domäne 30
Windows-Firewall 20

 Copyright © Acronis, Inc., 2000-2006

Lizenzvereinbarung

Acronis Privacy Expert 9.0 Corporate (Das SOFTWAREPRODUKT) unterliegt dem Copyright (C) 2000–2005 Acronis, Inc. Alle Rechte sind vorbehalten.

Der folgende Software-Lizenzvertrag ist jeder vertriebenen Kopie des lizenzierten SOFTWAREPRODUKTS beizufügen. Durch die Installation des SOFTWAREPRODUKTS nehmen Sie diesen Lizenzvertrag an und erklären, dass Sie ihn gelesen und verstanden haben und mit allen seinen Bedingungen einverstanden sind.

1. Lizenz

Acronis gewährt dem Käufer das nicht ausschließliche Recht, das SOFTWAREPRODUKT an einem Computer-Arbeitsplatz zu benutzen. Das Recht ist nicht übertragbar, vermietbar oder verleihbar. Es ist nicht gestattet, das SOFTWAREPRODUKT anderen Nutzern, die keine individuellen Lizenzen des SOFTWAREPRODUKTS besitzen, zur Nutzung im kommerziellen Computerservice, in Netzwerken, im Timesharing oder für Systeme mit mehreren Prozessoren bzw. mehreren Nutzern zur Verfügung zu stellen.

Das Kopieren und Archivieren des SOFTWAREPRODUKTS zum Zwecke der eigenen Datensicherung ist gestattet. Das Eigentum und die Urheberrechte oder sonstige Schutzrechte an dem SOFTWAREPRODUKT sowie den Dokumentationen, Handbüchern und Bedienungsanleitungen verbleiben nach wie vor bei Acronis.

2. Beschränkungen und Änderungsverbot

Das Programm oder Teile davon dürfen nicht kostenpflichtig oder kostenfrei weitergegeben, lizenziert, vermietet, verändert, übersetzt, angepasst oder veröffentlicht werden. Das SOFTWAREPRODUKT darf weder im Gesamten noch in Teilen disassembliert, dekompiliert oder auf andere Weise in allgemein lesbare Form zurückgewandelt werden.

3. Laufzeit des Vertrages

Die Lizenz gilt bis zu ihrer Beendigung. Der Lizenzvertrag kann dadurch beendet werden, dass das SOFTWAREPRODUKT sowie alle Kopien vernichtet werden. Die Lizenz erlischt unverzüglich, wenn gegen eine Bestimmung des Lizenzvertrags verstoßen wird, ohne dass es einer Kündigung durch Acronis, respektive seinen Lizenzpartnern, bedarf. Der ursprüngliche Käufer trägt gegenüber Acronis die Verantwortung für beliebige Schäden, die infolge einer Verletzung oder Nichtbeachtung des Lizenzvertrages entstehen.

4. Gewährleistungsausschluss und Haftung

Acronis haftet für die Dauer von 6 Monaten ab Übergabe des SOFTWAREPRODUKTS an Sie dafür, dass die CD-ROM, auf der das SOFTWAREPRODUKT gespeichert ist, frei von Mängeln ist, die die in der

Dokumentation ausgewiesene Nutzung erheblich mindern. Acronis gewährleistet nicht, dass das SOFTWAREPRODUKT fehlerfrei betrieben werden kann oder beliebige Defekte beseitigt, dass das SOFTWAREPRODUKT oder dessen Funktionen Ihren Anforderungen sowie dem von Ihnen gewünschten Einsatzzweck entsprechen. Acronis übernimmt keine Gewähr für die Vollständigkeit und Richtigkeit des Inhalts. Soweit nicht grob fahrlässiges oder vorsätzliches Verhalten vorliegt, übernehmen Acronis oder ihre Vertriebspartner keine Haftung für

- beliebige Verluste, die durch den Gebrauch des SOFTWAREPRODUKTS entstehen – einschließlich des Verlusts von Geschäftsgewinnen oder entgangenen Gewinnen in unbegrenzter Höhe
- Schäden an oder Verlust der gespeicherten Daten
- Geschäftsunterbrechung
- beliebige andere materielle oder immaterielle Verluste, die wegen der Benutzung oder der Verhinderung der Benutzung entstehen – selbst dann nicht, wenn Acronis oder ihre Vertriebspartner über die Möglichkeit derartiger Verluste in Kenntnis gesetzt wurden. Etwaige Schadensersatzansprüche sind unabhängig von der Anspruchsgrundlage in der Höhe auf die entrichtete Lizenzgebühr beschränkt.

Jegliche Ansprüche erlöschen in jedem Fall sechs Monate nach Lieferung.

5. Schlussbestimmungen

Es gilt deutsches Recht. Sollten einige Bestimmungen dieses Lizenzvertrages rechtlich unhaltbar oder unwirksam sein, bleiben alle anderen Bestimmungen rechtswirksam. Unwirksame Bestimmungen sind durch Regelungen zu ersetzen, die dem ursprünglichen Sinn am nächsten kommen.

 Copyright © Acronis, Inc., 2000-2006